E-Mail Header Information Results

Sender Information

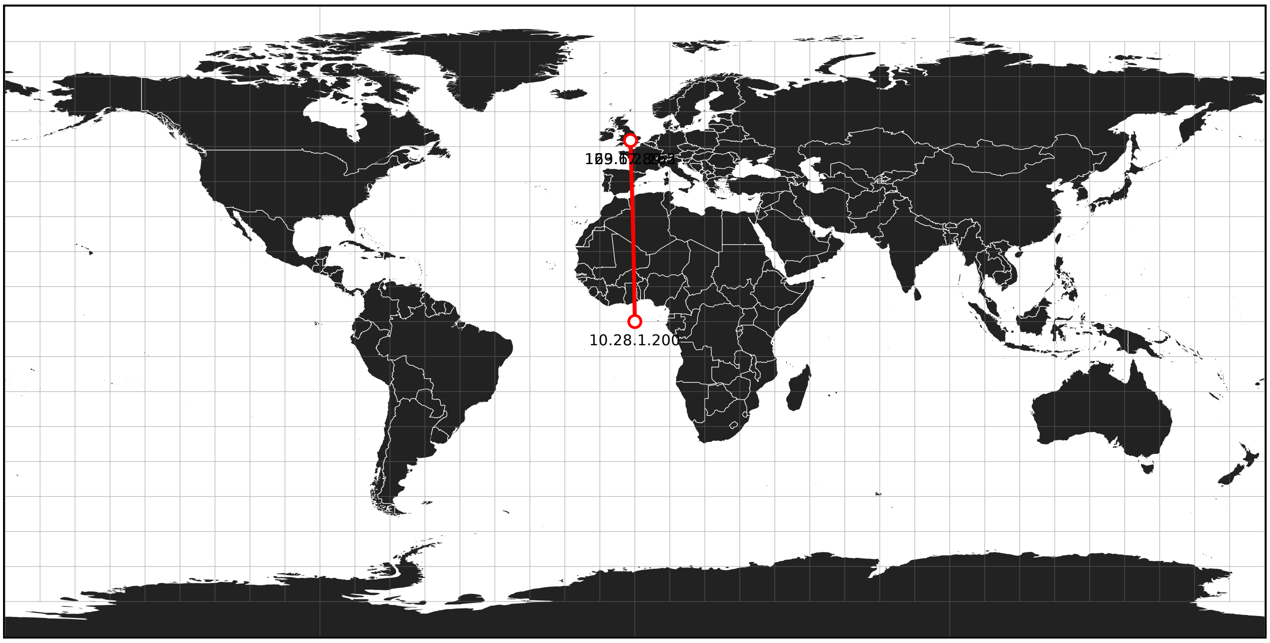
Name: Joshua Clark
Organisation: NOT FOUND

Sender Software

Software: Thunderbird

Found usernames

- *Oxford*
  sann4425

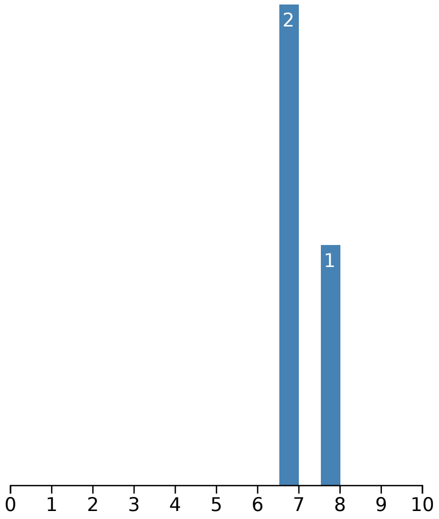


Class	Type	Details
Username	Username	sann4425
Application	Thunderbird	User-Agent
Personal	Sender Information	Joshua Clark

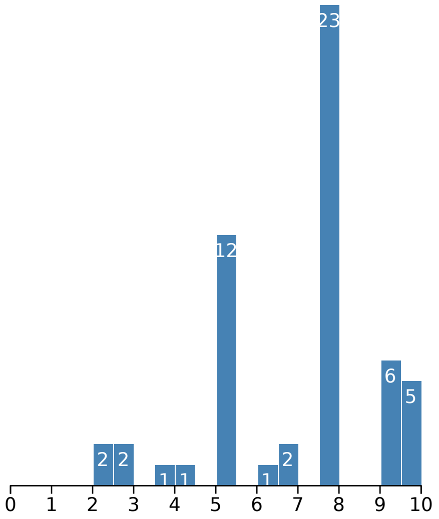
	Server	Time	Software	CVEs
0	10.28.1.200 (0,0)		SMTP	
1	(0,0)		ESMTPS	
2	163.1.2.162 (51.75,-1.25)		esmtp (Exim 4.80) (envelope-from)	
3	129.67.89.5 (51.75,-1.25)		esmtp (Exim 4.80) (envelope-from)	

Distribution of CVE Scores by Product

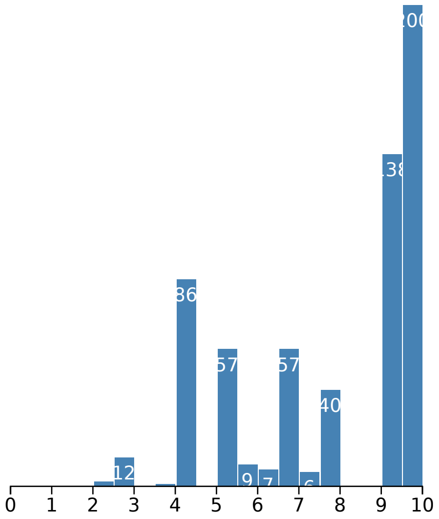
esmtp



smtp



thunderbird



Availability: Clear ▾ **Confidentiality:** Clear ▾ **Integrity:** Clear ▾ **Vector:** Clear ▾ **Complexity:** Clear ▾
Authentication: Clear ▾

Search

CVE-ID	Summary
CVE-2002-	The JavaScript implementation in Mozilla Firefox before 4.0, Thunderbird before 3.3, and SeaMonkey before 2.1 does not properly restrict the set of values contained in the object returned by the getComputedStyle method, which allows remote attackers to obtain

2437	sensitive information about visited web pages by calling this method.
CVE-2013-0791	The CERT_DecodeCertPackage function in Mozilla Network Security Services (NSS), as used in Mozilla Firefox before 20.0, Firefox ESR 17.x before 17.0.5, Thunderbird before 17.0.5, Thunderbird ESR 17.x before 17.0.5, SeaMonkey before 2.17, and other products, allows remote attackers to cause a denial of service (out-of-bounds read and memory corruption) via a crafted certificate.
CVE-2011-2605	CRLF injection vulnerability in the nsCookieService::SetCookieStringInternal function in netwerk/cookie/nsCookieService.cpp in Mozilla Firefox before 3.6.18 and 4.x through 4.0.1, and Thunderbird before 3.1.11, allows remote attackers to bypass intended access restrictions via a string containing a \n (newline) character, which is not properly handled in a JavaScript "document.cookie =" expression, a different vulnerability than CVE-2011-2374.
CVE-2013-0774	Mozilla Firefox before 19.0, Firefox ESR 17.x before 17.0.3, Thunderbird before 17.0.3, Thunderbird ESR 17.x before 17.0.3, and SeaMonkey before 2.16 do not prevent JavaScript workers from reading the browser-profile directory name, which has unspecified impact and remote attack vectors.
CVE-2010-0167	The browser engine in Mozilla Firefox 3.0.x before 3.0.18, 3.5.x before 3.5.8, and 3.6.x before 3.6.2; Thunderbird before 3.0.2; and SeaMonkey before 2.0.3 allows remote attackers to cause a denial of service (memory corruption and application crash) and possibly execute arbitrary code via vectors related to (1) layout/generic/nsBlockFrame.cpp and (2) the _evaluate function in modules/plugin/base/src/nsNPAPIPlugin.cpp.
CVE-2012-4186	Heap-based buffer overflow in the nsWaveReader::DecodeAudioData function in Mozilla Firefox before 16.0, Firefox ESR 10.x before 10.0.8, Thunderbird before 16.0, Thunderbird ESR 10.x before 10.0.8, and SeaMonkey before 2.13 allows remote attackers to execute arbitrary code via unspecified vectors.
CVE-2008-5500	The layout engine in Mozilla Firefox 3.x before 3.0.5 and 2.x before 2.0.0.19, Thunderbird 2.x before 2.0.0.19, and SeaMonkey 1.x before 1.1.14 allows remote attackers to cause a denial of service (crash) and possibly trigger memory corruption via vectors related to (1) a reachable assertion or (2) an integer overflow.
CVE-2011-2999	Mozilla Firefox before 3.6.23 and 4.x through 5, Thunderbird before 6.0, and SeaMonkey before 2.3 do not properly handle "location" as the name of a frame, which allows remote attackers to bypass the Same Origin Policy via a crafted web site, a different vulnerability than CVE-2010-0170.
CVE-2013-0758	Mozilla Firefox before 18.0, Firefox ESR 10.x before 10.0.12 and 17.x before 17.0.2, Thunderbird before 17.0.2, Thunderbird ESR 10.x before 10.0.12 and 17.x before 17.0.2, and SeaMonkey before 2.15 allow remote attackers to execute arbitrary JavaScript code with chrome privileges by leveraging improper interaction between plugin objects and SVG elements.
CVE-2005-2857	Free SMTP Server 2.2 allows remote attackers to use the server as an open mail relay (spam proxy).
CVE-2009-2535	Mozilla Firefox before 2.0.0.19 and 3.x before 3.0.5, SeaMonkey, and Thunderbird allow remote attackers to cause a denial of service (memory consumption and application crash) via a large integer value for the length property of a Select object, a related issue to CVE-2009-1692.
CVE-2008-2811	The block reflow implementation in Mozilla Firefox before 2.0.0.15, Thunderbird 2.0.0.14 and earlier, and SeaMonkey before 1.1.10 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via an image whose display requires more pixels than nscoord_MAX, related to nsBlockFrame::DrainOverflowLines.
CVE-2012-1939	jsinfer.cpp in Mozilla Firefox ESR 10.x before 10.0.5 and Thunderbird ESR 10.x before 10.0.5 does not properly determine data types, which allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via crafted JavaScript code.
CVE-2012-4216	Use-after-free vulnerability in the gfxFont::GetFontEntry function in Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0, Thunderbird ESR 10.x before 10.0.11, and SeaMonkey before 2.14 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2012-0475	Mozilla Firefox 4.x through 11.0, Thunderbird 5.0 through 11.0, and SeaMonkey before 2.9 do not properly construct the Origin and Sec-WebSocket-Origin HTTP headers, which might allow remote attackers to bypass an IPv6 literal ACL via a cross-site (1) XMLHttpRequest or (2) WebSocket operation involving a nonstandard port number and an IPv6 address that contains certain zero fields.
CVE-2013-0775	Use-after-free vulnerability in the nsImageLoadingContent::OnStopContainer function in Mozilla Firefox before 19.0, Firefox ESR 17.x before 17.0.3, Thunderbird before 17.0.3, Thunderbird ESR 17.x before 17.0.3, and SeaMonkey before 2.16 allows remote attackers to execute arbitrary code via crafted web script.
CVE-2007-5910	Stack-based buffer overflow in Autonomy (formerly Verity) KeyView Viewer, Filter, and Export SDK before 9.2.0.12, as used by ActivePDF DocConverter, wp6sr.dll in IBM Lotus Notes 8.0 and before 7.0.3, Symantec Mail Security, and other products, allows remote attackers to execute arbitrary code via a crafted WordPerfect (WPD) file.
CVE-2014-1578	The get_tile function in Mozilla Firefox before 33.0, Firefox ESR 31.x before 31.2, and Thunderbird 31.x before 31.2 allows remote attackers to cause a denial of service (out-of-bounds write and application crash) or possibly execute arbitrary code via WebM frames with invalid tile sizes that are improperly handled in buffering operations during video playback.
CVE-2012-3983	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 16.0, Thunderbird before 16.0, and SeaMonkey before 2.13 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2007-4841	Mozilla Firefox before 2.0.0.8, Thunderbird before 2.0.0.8, and SeaMonkey before 1.1.5 allows remote attackers to execute arbitrary commands via a (1) mailto, (2) nntp, (3) news, or (4) snews URI with invalid "%" encoding, related to improper file type handling on Windows XP with Internet Explorer 7 installed, a variant of CVE-2007-3845.
CVE-2012-1951	Use-after-free vulnerability in the nsSMILTimeValueSpec::IsEventBased function in Mozilla Firefox 4.x through 13.0, Firefox ESR 10.x before 10.0.6, Thunderbird 5.0 through 13.0, Thunderbird ESR 10.x before 10.0.6, and SeaMonkey before 2.11 allows remote attackers to cause a denial of service (heap memory corruption) or possibly execute arbitrary code by interacting with objects used for SMIL Timing.

CVE-2010-3768	Mozilla Firefox before 3.5.16 and 3.6.x before 3.6.13, Thunderbird before 3.0.11 and 3.1.x before 3.1.7, and SeaMonkey before 2.0.11 do not properly validate downloadable fonts before use within an operating system's font implementation, which allows remote attackers to execute arbitrary code via vectors related to @font-face Cascading Style Sheets (CSS) rules.
CVE-2012-1938	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 13.0, Thunderbird before 13.0, and SeaMonkey before 2.10 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to (1) methodjit/ImmutableSync.cpp, (2) the JSObject::makeDenseArraySlow function in js/src/jsarray.cpp, and unknown other components.
CVE-2011-3652	The browser engine in Mozilla Firefox before 8.0 and Thunderbird before 8.0 does not properly allocate memory, which allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unspecified vectors.
CVE-2014-1548	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 31.0 and Thunderbird before 31.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2012-0477	Multiple cross-site scripting (XSS) vulnerabilities in Mozilla Firefox 4.x through 11.0, Firefox ESR 10.x before 10.0.4, Thunderbird 5.0 through 11.0, Thunderbird ESR 10.x before 10.0.4, and SeaMonkey before 2.9 allow remote attackers to inject arbitrary web script or HTML via the (1) ISO-2022-KR or (2) ISO-2022-CN character set.
CVE-2012-4215	Use-after-free vulnerability in the nsPlaintextEditor::FireClipboardEvent function in Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0, Thunderbird ESR 10.x before 10.0.11, and SeaMonkey before 2.14 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2012-3957	Heap-based buffer overflow in the nsBlockFrame::MarkLineDirty function in Mozilla Firefox before 15.0, Firefox ESR 10.x before 10.0.7, Thunderbird before 15.0, Thunderbird ESR 10.x before 10.0.7, and SeaMonkey before 2.12 allows remote attackers to execute arbitrary code via unspecified vectors.
CVE-2012-1940	Use-after-free vulnerability in the nsFrameList::FirstChild function in Mozilla Firefox 4.x through 12.0, Firefox ESR 10.x before 10.0.5, Thunderbird 5.0 through 12.0, Thunderbird ESR 10.x before 10.0.5, and SeaMonkey before 2.10 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption and application crash) by changing the size of a container of absolutely positioned elements in a column.
CVE-2014-1505	The SVG filter implementation in Mozilla Firefox before 28.0, Firefox ESR 24.x before 24.4, Thunderbird before 24.4, and SeaMonkey before 2.25 allows remote attackers to obtain sensitive displacement-correlation information, and possibly bypass the Same Origin Policy and read text from a different domain, via a timing attack involving feDisplacementMap elements, a related issue to CVE-2013-1693.
CVE-2010-3170	Mozilla Firefox before 3.5.14 and 3.6.x before 3.6.11, Thunderbird before 3.0.9 and 3.1.x before 3.1.5, and SeaMonkey before 2.0.9 recognize a wildcard IP address in the subject's Common Name field of an X.509 certificate, which might allow man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority.
CVE-2011-2991	The browser engine in Mozilla Firefox 4.x through 5, SeaMonkey 2.x before 2.3, Thunderbird before 6, and possibly other products does not properly implement JavaScript, which allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unspecified vectors.
CVE-2013-0773	The Chrome Object Wrapper (COW) and System Only Wrapper (SOW) implementations in Mozilla Firefox before 19.0, Firefox ESR 17.x before 17.0.3, Thunderbird before 17.0.3, Thunderbird ESR 17.x before 17.0.3, and SeaMonkey before 2.16 do not prevent modifications to a prototype, which allows remote attackers to obtain sensitive information from chrome objects or possibly execute arbitrary JavaScript code with chrome privileges via a crafted web site.
CVE-2011-2376	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 3.6.18 and Thunderbird before 3.1.11 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2011-3653	Mozilla Firefox before 8.0 and Thunderbird before 8.0 on Mac OS X do not properly interact with the GPU memory behavior of a certain driver for Intel integrated GPUs, which allows remote attackers to bypass the Same Origin Policy and read image data via vectors related to WebGL textures.
CVE-2013-0759	Mozilla Firefox before 18.0, Firefox ESR 10.x before 10.0.12 and 17.x before 17.0.2, Thunderbird before 17.0.2, Thunderbird ESR 10.x before 10.0.12 and 17.x before 17.0.2, and SeaMonkey before 2.15 allow remote attackers to spoof the address bar via vectors involving authentication information in the userinfo field of a URL, in conjunction with a 204 (aka No Content) HTTP status code.
CVE-2012-0473	The WebGLBuffer::FindMaxUshortElement function in Mozilla Firefox 4.x through 11.0, Firefox ESR 10.x before 10.0.4, Thunderbird 5.0 through 11.0, Thunderbird ESR 10.x before 10.0.4, and SeaMonkey before 2.9 calls the FindMaxElementInSubArray function with incorrect template arguments, which allows remote attackers to obtain sensitive information from video memory via a crafted WebGL.drawElements call.
CVE-2012-4185	Buffer overflow in the nsCharTraits::length function in Mozilla Firefox before 16.0, Firefox ESR 10.x before 10.0.8, Thunderbird before 16.0, Thunderbird ESR 10.x before 10.0.8, and SeaMonkey before 2.13 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2012-4201	The evalInSandbox implementation in Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0, Thunderbird ESR 10.x before 10.0.11, and SeaMonkey before 2.14 uses an incorrect context during the handling of JavaScript code that sets the location.href property, which allows remote attackers to conduct cross-site scripting (XSS) attacks or read arbitrary files by leveraging a sandboxed add-on.
CVE-2013-1701	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 23.0, Firefox ESR 17.x before 17.0.8, Thunderbird before 17.0.8, Thunderbird ESR 17.x before 17.0.8, and SeaMonkey before 2.20 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2010-3769	The line-breaking implementation in Mozilla Firefox before 3.5.16 and 3.6.x before 3.6.13, Thunderbird before 3.0.11 and 3.1.x before 3.1.7, and SeaMonkey before 2.0.11 on Windows does not properly handle long strings, which allows remote attackers to execute arbitrary code via a crafted document.write call that triggers a buffer over-read.

CVE-2014-1550	Use-after-free vulnerability in the MediaInputPort class in Mozilla Firefox before 31.0 and Thunderbird before 31.0 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) by leveraging incorrect Web Audio control-message ordering.
CVE-2008-3835	The nsXMLDocument::OnChannelRedirect function in Mozilla Firefox before 2.0.0.17, Thunderbird before 2.0.0.17, and SeaMonkey before 1.1.12 allows remote attackers to bypass the Same Origin Policy and execute arbitrary JavaScript code via unknown vectors.
CVE-2013-0788	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 20.0, Firefox ESR 17.x before 17.0.5, Thunderbird before 17.0.5, Thunderbird ESR 17.x before 17.0.5, and SeaMonkey before 2.17 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2011-3000	Mozilla Firefox before 3.6.23 and 4.x through 6, Thunderbird before 7.0, and SeaMonkey before 2.4 do not properly handle HTTP responses that contain multiple Location, Content-Length, or Content-Disposition headers, which makes it easier for remote attackers to conduct HTTP response splitting attacks via crafted header values.
CVE-2010-3131	Untrusted search path vulnerability in Mozilla Firefox before 3.5.12 and 3.6.x before 3.6.9, Thunderbird before 3.0.7 and 3.1.x before 3.1.3, and SeaMonkey before 2.0.7 on Windows XP allows local users, and possibly remote attackers, to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse dwmapi.dll that is located in the same folder as a .htm, .html, .jtx, .mfp, or .eml file.
CVE-2014-1581	Use-after-free vulnerability in DirectionalityUtils.cpp in Mozilla Firefox before 33.0, Firefox ESR 31.x before 31.2, and Thunderbird 31.x before 31.2 allows remote attackers to execute arbitrary code via text that is improperly handled during the interaction between directionality resolution and layout.
CVE-2014-1567	Use-after-free vulnerability in DirectionalityUtils.cpp in Mozilla Firefox before 32.0, Firefox ESR 24.x before 24.8 and 31.x before 31.1, and Thunderbird 24.x before 24.8 and 31.x before 31.1 allows remote attackers to execute arbitrary code via text that is improperly handled during the interaction between directionality resolution and layout.
CVE-2011-2992	The Ogg reader in the browser engine in Mozilla Firefox 4.x through 5, SeaMonkey 2.x before 2.3, Thunderbird before 6, and possibly other products allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unspecified vectors.
CVE-2013-0760	Buffer overflow in the CharDistributionAnalysis::HandleOneChar function in Mozilla Firefox before 18.0, Thunderbird before 17.0.2, and SeaMonkey before 2.15 allows remote attackers to execute arbitrary code via a crafted document.
CVE-2015-2736	The nsZipArchive::BuildFileList function in Mozilla Firefox before 39.0, Firefox ESR 31.x before 31.8 and 38.x before 38.1, and Thunderbird before 38.1 accesses unintended memory locations, which allows remote attackers to have an unspecified impact via a crafted ZIP archive.
CVE-2012-0474	Cross-site scripting (XSS) vulnerability in the docshell implementation in Mozilla Firefox 4.x through 11.0, Firefox ESR 10.x before 10.0.4, Thunderbird 5.0 through 11.0, Thunderbird ESR 10.x before 10.0.4, and SeaMonkey before 2.9 allows remote attackers to inject arbitrary web script or HTML via vectors related to short-circuited page loads, aka "Universal XSS (UXSS)."
CVE-2012-4217	Use-after-free vulnerability in the nsViewManager::ProcessPendingUpdates function in Mozilla Firefox before 17.0, Thunderbird before 17.0, and SeaMonkey before 2.14 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2012-3956	Use-after-free vulnerability in the MediaStreamGraphThreadRunnable::Run function in Mozilla Firefox before 15.0, Firefox ESR 10.x before 10.0.7, Thunderbird before 15.0, Thunderbird ESR 10.x before 10.0.7, and SeaMonkey before 2.12 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2013-1697	The XrayWrapper implementation in Mozilla Firefox before 22.0, Firefox ESR 17.x before 17.0.7, Thunderbird before 17.0.7, and Thunderbird ESR 17.x before 17.0.7 does not properly restrict use of DefaultValue for method calls, which allows remote attackers to execute arbitrary JavaScript code with chrome privileges via a crafted web site that triggers use of a user-defined (1) toString or (2) valueOf method.
CVE-2015-0831	Use-after-free vulnerability in the mozilla::dom::IndexedDB::IDBObjectStore::CreateIndex function in Mozilla Firefox before 36.0, Firefox ESR 31.x before 31.5, and Thunderbird before 31.5 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via crafted content that is improperly handled during IndexedDB index creation.
CVE-2012-5836	Mozilla Firefox before 17.0, Thunderbird before 17.0, and SeaMonkey before 2.14 allow remote attackers to execute arbitrary code or cause a denial of service (application crash) via vectors involving the setting of Cascading Style Sheets (CSS) properties in conjunction with SVG text.
CVE-2014-1590	The XMLHttpRequest.prototype.send method in Mozilla Firefox before 34.0, Firefox ESR 31.x before 31.3, Thunderbird before 31.3, and SeaMonkey before 2.31 allows remote attackers to cause a denial of service (application crash) via a crafted JavaScript object.
CVE-2012-3980	The web console in Mozilla Firefox before 15.0, Firefox ESR 10.x before 10.0.7, Thunderbird before 15.0, and Thunderbird ESR 10.x before 10.0.7 allows user-assisted remote attackers to execute arbitrary JavaScript code with chrome privileges via a crafted web site that injects this code and triggers an eval operation.
CVE-2012-1952	The nsTableFrame::InsertFrames function in Mozilla Firefox 4.x through 13.0, Firefox ESR 10.x before 10.0.6, Thunderbird 5.0 through 13.0, Thunderbird ESR 10.x before 10.0.6, and SeaMonkey before 2.11 does not properly perform a cast of a frame variable during processing of mixed row-group and column-group frames, which might allow remote attackers to execute arbitrary code via a crafted web site.
CVE-2011-2377	Mozilla Firefox before 3.6.18 and 4.x through 4.0.1, Thunderbird before 3.1.11, and SeaMonkey through 2.0.14 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via a multipart/x-mixed-replace image.
CVE-2007-6020	Multiple stack-based buffer overflows in foliosr.dll in the Folio Flat File speed reader in Autonomy (formerly Verity) KeyView 10.3.0.0, as used by IBM Lotus Notes, Symantec Mail Security, and activePDF DocConverter, allow remote attackers to execute arbitrary code via a long attribute value in a (1) DI, (2) FD, (3) FT, (4) JD, (5) JL, (6) LE, (7) OB, (8) OD, (9) OL, (10) PN, (11) PS, (12) PW, (13) RD, (14) QL, or

	(15) TS tag in a .fff file.
CVE-2016-1974	The nsScannerString::AppendUnicodeTo function in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7 does not verify that memory allocation succeeds, which allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds read) via crafted Unicode data in an HTML, XML, or SVG document.
CVE-2014-1549	The mozilla::dom::AudioBufferSourceNodeEngine::CopyFromInputBuffer function in Mozilla Firefox before 31.0 and Thunderbird before 31.0 does not properly allocate Web Audio buffer memory, which allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via crafted audio content that is improperly handled during playback buffering.
CVE-2013-6671	The nsGfxScrollFrameInner::IsLTR function in Mozilla Firefox before 26.0, Firefox ESR 24.x before 24.2, Thunderbird before 24.2, and SeaMonkey before 2.23 allows remote attackers to execute arbitrary code via crafted use of JavaScript code for ordered list elements.
CVE-2012-4184	The Chrome Object Wrapper (COW) implementation in Mozilla Firefox before 16.0, Firefox ESR 10.x before 10.0.8, Thunderbird before 16.0, Thunderbird ESR 10.x before 10.0.8, and SeaMonkey before 2.13 does not prevent access to properties of a prototype for a standard class, which allows remote attackers to execute arbitrary JavaScript code with chrome privileges via a crafted web site.
CVE-2014-1496	Mozilla Firefox before 28.0, Firefox ESR 24.x before 24.4, Thunderbird before 24.4, and SeaMonkey before 2.25 might allow local users to gain privileges by modifying the extracted Mar contents during an update.
CVE-2008-5018	The JavaScript engine in Mozilla Firefox 3.x before 3.0.4, Firefox 2.x before 2.0.0.18, Thunderbird 2.x before 2.0.0.18, and SeaMonkey 1.x before 1.1.13 allows remote attackers to cause a denial of service (crash) via vectors related to "insufficient class checking" in the Date class.
CVE-2012-4183	Use-after-free vulnerability in the DOMSVGTests::GetRequiredFeatures function in Mozilla Firefox before 16.0, Firefox ESR 10.x before 10.0.8, Thunderbird before 16.0, Thunderbird ESR 10.x before 10.0.8, and SeaMonkey before 2.13 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2011-3654	The browser engine in Mozilla Firefox before 8.0 and Thunderbird before 8.0 does not properly handle links from SVG mpath elements to non-SVG elements, which allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unspecified vectors.
CVE-2009-0773	The JavaScript engine in Mozilla Firefox before 3.0.7, Thunderbird before 2.0.0.21, and SeaMonkey 1.1.15 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via (1) a splice of an array that contains "some non-set elements," which causes jsarray.cpp to pass an incorrect argument to the ResizeSlots function, which triggers memory corruption; (2) vectors related to js_DecompileValueGenerator, jsopcode.cpp, __defineSetter__, and watch, which triggers an assertion failure or a segmentation fault; and (3) vectors related to gczeal, __defineSetter__, and watch, which triggers a hang.
CVE-2005-1346	Multiple Symantec AntiVirus products, including Norton AntiVirus 2005 11.0.0, Web Security Web Security 3.0.1.72, Mail Security for SMTP 4.0.5.66, AntiVirus Scan Engine 4.3.7.27, SAV/Filter for Domino NT 3.1.1.87, and Mail Security for Exchange 4.5.4.743, when running on Windows, allows remote attackers to cause a denial of service (component crash) and avoid detection via a crafted RAR file.
CVE-2012-1948	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 4.x through 13.0, Firefox ESR 10.x before 10.0.6, Thunderbird 5.0 through 13.0, Thunderbird ESR 10.x before 10.0.6, and SeaMonkey before 2.11 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2013-5591	Unspecified vulnerability in the browser engine in Mozilla Firefox before 25.0, Firefox ESR 24.x before 24.1, Thunderbird before 24.1, and SeaMonkey before 2.22 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2010-3183	The LookupGetterOrSetter function in js3250.dll in Mozilla Firefox before 3.5.14 and 3.6.x before 3.6.11, Thunderbird before 3.0.9 and 3.1.x before 3.1.5, and SeaMonkey before 2.0.9 does not properly support window.__lookupGetter__ function calls that lack arguments, which allows remote attackers to execute arbitrary code or cause a denial of service (incorrect pointer dereference and application crash) via vectors involving a "dangling pointer" and the JS_ValueToId function.
CVE-1999-1200	Vintra SMTP MailServer allows remote attackers to cause a denial of service via a malformed "EXPN *@" command.
CVE-2012-1942	The Mozilla Updater and Windows Updater Service in Mozilla Firefox 12.0, Thunderbird 12.0, and SeaMonkey 2.9 on Windows allow local users to gain privileges by loading a DLL file in a privileged context.
CVE-2010-3173	The SSL implementation in Mozilla Firefox before 3.5.14 and 3.6.x before 3.6.11, Thunderbird before 3.0.9 and 3.1.x before 3.1.5, and SeaMonkey before 2.0.9 does not properly set the minimum key length for Diffie-Hellman Ephemeral (DHE) mode, which makes it easier for remote attackers to defeat cryptographic protection mechanisms via a brute-force attack.
CVE-2007-0777	The JavaScript engine in Mozilla Firefox before 1.5.0.10 and 2.x before 2.0.0.2, Thunderbird before 1.5.0.10, and SeaMonkey before 1.0.8 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via certain vectors that trigger memory corruption.
CVE-2012-0472	The cairo-dwrite implementation in Mozilla Firefox 4.x through 11.0, Firefox ESR 10.x before 10.0.4, Thunderbird 5.0 through 11.0, Thunderbird ESR 10.x before 10.0.4, and SeaMonkey before 2.9, when certain Windows Vista and Windows 7 configurations are used, does not properly restrict font-rendering attempts, which allows remote attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors.
CVE-2012-3982	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 16.0, Firefox ESR 10.x before 10.0.8, Thunderbird before 16.0, Thunderbird ESR 10.x before 10.0.8, and SeaMonkey before 2.13 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2008-4058	The XPConnect component in Mozilla Firefox before 2.0.0.17 and 3.x before 3.0.2, Thunderbird before 2.0.0.17, and SeaMonkey before 1.1.12 allows remote attackers to "pollute XPCNativeWrappers" and execute arbitrary code with chrome privileges via vectors related to (1) chrome XBL and (2) chrome JS.

CVE-2012-1941	Heap-based buffer overflow in the nsHTMLReflowState::CalculateHypotheticalBox function in Mozilla Firefox 4.x through 12.0, Firefox ESR 10.x before 10.0.5, Thunderbird 5.0 through 12.0, Thunderbird ESR 10.x before 10.0.5, and SeaMonkey before 2.10 allows remote attackers to execute arbitrary code by resizing a window displaying absolutely positioned and relatively positioned elements in nested columns.
CVE-2014-1518	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 29.0, Firefox ESR 24.x before 24.5, Thunderbird before 24.5, and SeaMonkey before 2.26 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2012-5838	The copyTexImage2D implementation in the WebGL subsystem in Mozilla Firefox before 17.0, Thunderbird before 17.0, and SeaMonkey before 2.14 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via large image dimensions.
CVE-2008-5021	nsFrameManager in Firefox 3.x before 3.0.4, Firefox 2.x before 2.0.0.18, Thunderbird 2.x before 2.0.0.18, and SeaMonkey 1.x before 1.1.13 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code by modifying properties of a file input element while it is still being initialized, then using the blur method to access uninitialized memory.
CVE-2004-0156	Format string vulnerabilities in the (1) die or (2) log_event functions for ssmtp before 2.50.6 allow remote mail relays to cause a denial of service and possibly execute arbitrary code.
CVE-2012-3958	Use-after-free vulnerability in the nsHTMLEditRules::DeleteNonTableElements function in Mozilla Firefox before 15.0, Firefox ESR 10.x before 10.0.7, Thunderbird before 15.0, Thunderbird ESR 10.x before 10.0.7, and SeaMonkey before 2.12 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2008-5506	Mozilla Firefox 3.x before 3.0.5 and 2.x before 2.0.0.19, Thunderbird 2.x before 2.0.0.19, and SeaMonkey 1.x before 1.1.14 allows remote attackers to bypass the same origin policy by causing the browser to issue an XMLHttpRequest to an attacker-controlled resource that uses a 302 redirect to a resource in a different domain, then reading content from the response, aka "response disclosure."
CVE-2011-3666	Mozilla Firefox before 3.6.25 and Thunderbird before 3.1.17 on Mac OS X do not consider .jar files to be executable files, which allows user-assisted remote attackers to bypass intended access restrictions via a crafted file. NOTE: this vulnerability exists because of an incorrect fix for CVE-2011-2372 on Mac OS X.
CVE-2012-4193	Mozilla Firefox before 16.0.1, Firefox ESR 10.x before 10.0.9, Thunderbird before 16.0.1, Thunderbird ESR 10.x before 10.0.9, and SeaMonkey before 2.13.1 omit a security check in the defaultValue function during the unwrapping of security wrappers, which allows remote attackers to bypass the Same Origin Policy and read the properties of a Location object, or execute arbitrary JavaScript code, via a crafted web site.
CVE-2013-0755	Use-after-free vulnerability in the mozVibrate implementation in the Vibrate library in Mozilla Firefox before 18.0, Firefox ESR 17.x before 17.0.2, Thunderbird before 17.0.2, Thunderbird ESR 17.x before 17.0.2, and SeaMonkey before 2.15 allows remote attackers to execute arbitrary code via vectors related to the domDoc pointer.
CVE-2008-3962	The from_format function in ssmtp.c in ssmtp 2.61 and 2.62, in certain configurations, uses uninitialized memory for the From: field of an e-mail message, which might allow remote attackers to obtain sensitive information (memory contents) in opportunistic circumstances by reading a message.
CVE-2009-0771	The layout engine in Mozilla Firefox before 3.0.7, Thunderbird before 2.0.0.21, and SeaMonkey 1.1.15 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via certain vectors that trigger memory corruption and assertion failures.
CVE-2012-4218	Use-after-free vulnerability in the BuildTextRunsScanner::BreakSink::SetBreaks function in Mozilla Firefox before 17.0, Thunderbird before 17.0, and SeaMonkey before 2.14 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2012-0464	Use-after-free vulnerability in the browser engine in Mozilla Firefox before 3.6.28 and 4.x through 10.0, Firefox ESR 10.x before 10.0.3, Thunderbird before 3.1.20 and 5.0 through 10.0, Thunderbird ESR 10.x before 10.0.3, and SeaMonkey before 2.8 allows remote attackers to execute arbitrary code via vectors involving an empty argument to the array.join function in conjunction with the triggering of garbage collection.
CVE-2014-1544	Use-after-free vulnerability in the CERT_DestroyCertificate function in libnss3.so in Mozilla Network Security Services (NSS) 3.x, as used in Firefox before 31.0, Firefox ESR 24.x before 24.7, and Thunderbird before 24.7, allows remote attackers to execute arbitrary code via vectors that trigger certain improper removal of an NSSCertificate structure from a trust domain.
CVE-2014-1477	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 27.0, Firefox ESR 24.x before 24.3, Thunderbird before 24.3, and SeaMonkey before 2.24 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2010-0159	The browser engine in Mozilla Firefox 3.0.x before 3.0.18 and 3.5.x before 3.5.8, Thunderbird before 3.0.2, and SeaMonkey before 2.0.3 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to the nsBlockFrame::StealFrame function in layout/generic/nsBlockFrame.cpp, and unspecified other vectors.
CVE-2013-5593	The SELECT element implementation in Mozilla Firefox before 25.0, Firefox ESR 24.x before 24.1, Thunderbird before 24.1, and SeaMonkey before 2.22 does not properly restrict the nature or placement of HTML within a dropdown menu, which allows remote attackers to spoof the address bar or conduct clickjacking attacks via vectors that trigger navigation off of a page containing this element.
CVE-2010-0169	The CSSLoaderImpl::DoSheetComplete function in layout/style/nsCSSLoader.cpp in Mozilla Firefox 3.0.x before 3.0.18, 3.5.x before 3.5.8, and 3.6.x before 3.6.2; Thunderbird before 3.0.2; and SeaMonkey before 2.0.3 changes the case of certain strings in a stylesheet before adding this stylesheet to the XUL cache, which might allow remote attackers to modify the browser's font and other CSS attributes, and potentially disrupt rendering of a web page, by forcing the browser to perform this erroneous stylesheet caching.
CVE-2006-	Format string vulnerability in the SMTP server for McAfee WebShield 4.5 MR2 and earlier allows remote attackers to execute arbitrary code via format strings in the domain name portion of a destination address, which are not properly handled when a bounce message

0559	is constructed.
CVE-2004-0648	Mozilla (Suite) before 1.7.1, Firefox before 0.9.2, and Thunderbird before 0.7.2 allow remote attackers to launch arbitrary programs via a URI referencing the shell: protocol.
CVE-2014-1493	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 28.0, Firefox ESR 24.x before 24.4, Thunderbird before 24.4, and SeaMonkey before 2.25 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2009-0772	The layout engine in Mozilla Firefox 2 and 3 before 3.0.7, Thunderbird before 2.0.0.21, and SeaMonkey 1.1.15 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via vectors related to nsCSSStyleSheet::GetOwnerNode, events, and garbage collection, which triggers memory corruption.
CVE-2008-5022	The nsXMLHttpRequest::NotifyEventListeners method in Firefox 3.x before 3.0.4, Firefox 2.x before 2.0.0.18, Thunderbird 2.x before 2.0.0.18, and SeaMonkey 1.x before 1.1.13 allows remote attackers to bypass the same-origin policy and execute arbitrary script via multiple listeners, which bypass the inner window check.
CVE-2012-1943	Untrusted search path vulnerability in Updater.exe in the Windows Updater Service in Mozilla Firefox 12.0, Thunderbird 12.0, and SeaMonkey 2.9 on Windows allows local users to gain privileges via a Trojan horse wsock32.dll file in an application directory.
CVE-2015-0813	Use-after-free vulnerability in the AppendElements function in Mozilla Firefox before 37.0, Firefox ESR 31.x before 31.6, and Thunderbird before 31.6 on Linux, when the Fluendo MP3 plugin for GStreamer is used, allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via a crafted MP3 file.
CVE-2014-1547	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 31.0, Firefox ESR 24.x before 24.7, and Thunderbird before 24.7 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2012-0470	Heap-based buffer overflow in the nsSVGFEDiffuseLightingElement::LightPixel function in Mozilla Firefox 4.x through 11.0, Firefox ESR 10.x before 10.0.4, Thunderbird 5.0 through 11.0, Thunderbird ESR 10.x before 10.0.4, and SeaMonkey before 2.9 allows remote attackers to cause a denial of service (invalid gfxImageSurface free operation) or possibly execute arbitrary code by leveraging the use of "different number systems."
CVE-2008-5501	The layout engine in Mozilla Firefox 3.x before 3.0.5, Thunderbird 2.x before 2.0.0.19, and SeaMonkey 1.x before 1.1.14 allows remote attackers to cause a denial of service via vectors that trigger an assertion failure.
CVE-2013-0756	Use-after-free vulnerability in the obj_toSource function in Mozilla Firefox before 18.0, Firefox ESR 17.x before 17.0.2, Thunderbird before 17.0.2, Thunderbird ESR 17.x before 17.0.2, and SeaMonkey before 2.15 allows remote attackers to execute arbitrary code via a crafted web page referencing JavaScript Proxy objects that are not properly handled during garbage collection.
CVE-2012-4182	Use-after-free vulnerability in the nsTextEditRules::WillInsert function in Mozilla Firefox before 16.0, Firefox ESR 10.x before 10.0.8, Thunderbird before 16.0, Thunderbird ESR 10.x before 10.0.8, and SeaMonkey before 2.13 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2010-3169	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 3.5.12 and 3.6.x before 3.6.9, Thunderbird before 3.0.7 and 3.1.x before 3.1.3, and SeaMonkey before 2.0.7 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2013-0772	The RasterImage::DrawFrameTo function in Mozilla Firefox before 19.0, Thunderbird before 17.0.3, and SeaMonkey before 2.16 allows remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read and application crash) via a crafted GIF image.
CVE-2010-0173	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 3.5.9 and 3.6.x before 3.6.2, Thunderbird before 3.0.4, and SeaMonkey before 2.0.4 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2012-1949	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 4.x through 13.0, Thunderbird 5.0 through 13.0, and SeaMonkey before 2.11 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2011-2997	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 6, Thunderbird before 7.0, and SeaMonkey before 2.4 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2015-2729	The AudioParamTimeline::AudioNodeInputValue function in the Web Audio implementation in Mozilla Firefox before 39.0 and Firefox ESR 38.x before 38.1 does not properly calculate an oscillator rendering range, which allows remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2012-5840	Use-after-free vulnerability in the nsTextEditorState::PrepareEditor function in Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0, Thunderbird ESR 10.x before 10.0.11, and SeaMonkey before 2.14 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors, a different vulnerability than CVE-2012-4214.
CVE-2011-3665	Mozilla Firefox 4.x through 8.0, Thunderbird 5.0 through 8.0, and SeaMonkey before 2.6 allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via an Ogg VIDEO element that is not properly handled after scaling.
CVE-2013-1707	Stack-based buffer overflow in Mozilla Updater in Mozilla Firefox before 23.0, Firefox ESR 17.x before 17.0.8, Thunderbird before 17.0.8, and Thunderbird ESR 17.x before 17.0.8 allows local users to gain privileges via a long pathname on the command line to the Mozilla Maintenance Service.
CVE-2015-	Multiple untrusted search path vulnerabilities in updater.exe in Mozilla Firefox before 36.0, Firefox ESR 31.x before 31.5, and Thunderbird before 31.5 on Windows, when the Maintenance Service is not used, allow local users to gain privileges via a Trojan horse

0833	DLL in (1) the current working directory or (2) a temporary directory, as demonstrated by bcrypt.dll.
CVE-2006-4258	Absolute path traversal vulnerability in the get functionality in Anti-Spam SMTP Proxy (ASSP) allows remote authenticated users to read arbitrary files via (1) C:\ (Windows drive letter), (2) UNC, and possibly other types of paths in the file parameter.
CVE-2006-0884	The WYSIWYG rendering engine ("rich mail" editor) in Mozilla Thunderbird 1.0.7 and earlier allows user-assisted attackers to bypass javascript security settings and obtain sensitive information or cause a crash via an e-mail containing a javascript URI in the SRC attribute of an IFRAME tag, which is executed when the user edits the e-mail.
CVE-2015-0822	The Form Autocompletion feature in Mozilla Firefox before 36.0, Firefox ESR 31.x before 31.5, and Thunderbird before 31.5 allows remote attackers to read arbitrary files via crafted JavaScript code.
CVE-2008-4060	Mozilla Firefox before 2.0.0.17 and 3.x before 3.0.2, Thunderbird before 2.0.0.17, and SeaMonkey before 1.1.12 allow remote attackers to create documents that lack script-handling objects, and execute arbitrary code with chrome privileges, via vectors related to (1) the document.loadBindingDocument function and (2) XSLT.
CVE-2011-3655	Mozilla Firefox 4.x through 7.0 and Thunderbird 5.0 through 7.0 perform access control without checking for use of the NoWaiverWrapper wrapper, which allows remote attackers to gain privileges via a crafted web site.
CVE-2008-5503	The loadBindingDocument function in Mozilla Firefox 2.x before 2.0.0.19, Thunderbird 2.x before 2.0.0.19, and SeaMonkey 1.x before 1.1.14 does not perform any security checks related to the same-domain policy, which allows remote attackers to read or access data from other domains via crafted XBL bindings.
CVE-2014-1497	The mozilla::WaveReader::DecodeAudioData function in Mozilla Firefox before 28.0, Firefox ESR 24.x before 24.4, Thunderbird before 24.4, and SeaMonkey before 2.25 allows remote attackers to obtain sensitive information from process heap memory, cause a denial of service (out-of-bounds read and application crash), or possibly have unspecified other impact via a crafted WAV file.
CVE-2010-3174	Unspecified vulnerability in the browser engine in Mozilla Firefox 3.5.x before 3.5.14, Thunderbird before 3.0.9, and SeaMonkey before 2.0.9 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2010-3168	Mozilla Firefox before 3.5.12 and 3.6.x before 3.6.9, Thunderbird before 3.0.7 and 3.1.x before 3.1.3, and SeaMonkey before 2.0.7 do not properly restrict the role of property changes in triggering XUL tree removal, which allows remote attackers to cause a denial of service (deleted memory access and application crash) or possibly execute arbitrary code by setting unspecified properties.
CVE-2010-0171	Mozilla Firefox 3.0.x before 3.0.18, 3.5.x before 3.5.8, and 3.6.x before 3.6.2; Thunderbird before 3.0.2; and SeaMonkey before 2.0.3 allow remote attackers to perform cross-origin keystroke capture, and possibly conduct cross-site scripting (XSS) attacks, by using the addEventListener and setTimeout functions in conjunction with a wrapped object. NOTE: this vulnerability exists because of an incomplete fix for CVE-2007-3736.
CVE-2012-0471	Cross-site scripting (XSS) vulnerability in Mozilla Firefox 4.x through 11.0, Firefox ESR 10.x before 10.0.4, Thunderbird 5.0 through 11.0, Thunderbird ESR 10.x before 10.0.4, and SeaMonkey before 2.9 allows remote attackers to inject arbitrary web script or HTML via a multibyte character set.
CVE-2008-4061	Integer overflow in the MathML component in Mozilla Firefox before 2.0.0.17 and 3.x before 3.0.2, Thunderbird before 2.0.0.17, and SeaMonkey before 1.1.12 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via an mtd element with a large integer value in the rowspan attribute, related to the layout engine.
CVE-2010-0163	Mozilla Thunderbird before 2.0.0.24 and SeaMonkey before 1.1.19 process e-mail attachments with a parser that performs casts and line termination incorrectly, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted message, related to message indexing.
CVE-2013-1706	Stack-based buffer overflow in maintenanceservice.exe in the Mozilla Maintenance Service in Mozilla Firefox before 23.0, Firefox ESR 17.x before 17.0.8, Thunderbird before 17.0.8, and Thunderbird ESR 17.x before 17.0.8 allows local users to gain privileges via a long pathname on the command line.
CVE-2011-3664	Mozilla Firefox before 9.0, Thunderbird before 9.0, and SeaMonkey before 2.6 on Mac OS X do not properly handle certain DOM frame deletions by plugins, which allows remote attackers to cause a denial of service (incorrect pointer dereference and application crash) or possibly have unspecified other impact via a crafted web site.
CVE-2012-4202	Heap-based buffer overflow in the image::RasterImage::DrawFrameTo function in Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0, Thunderbird ESR 10.x before 10.0.11, and SeaMonkey before 2.14 allows remote attackers to execute arbitrary code via a crafted GIF image.
CVE-2008-5024	Mozilla Firefox 3.x before 3.0.4, Firefox 2.x before 2.0.0.18, Thunderbird 2.x before 2.0.0.18, and SeaMonkey 1.x before 1.1.13 do not properly escape quote characters used for XML processing, which allows remote attackers to conduct XML injection attacks via the default namespace in an E4X document.
CVE-2012-5839	Heap-based buffer overflow in the gfxShapedWord::CompressedGlyph::IsClusterStart function in Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0, Thunderbird ESR 10.x before 10.0.11, and SeaMonkey before 2.14 allows remote attackers to execute arbitrary code via unspecified vectors.
CVE-2013-2125	OpenSMTPD before 5.3.2 does not properly handle SSL sessions, which allows remote attackers to cause a denial of service (connection blocking) by keeping a connection open.
CVE-2008-5502	The layout engine in Mozilla Firefox 3.x before 3.0.5, Thunderbird 2.x before 2.0.0.19, and SeaMonkey 1.x before 1.1.14 allows remote attackers to cause a denial of service (crash) via vectors that trigger memory corruption, related to the GetXMLEntity and FastAppendChar functions.
CVE-	Use-after-free vulnerability in the nsRangeUpdater::SelAdjDeleteNode function in Mozilla Firefox before 15.0, Firefox ESR 10.x before

2012-3959	10.0.7, Thunderbird before 15.0, Thunderbird ESR 10.x before 10.0.7, and SeaMonkey before 2.12 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2013-0757	The Chrome Object Wrapper (COW) implementation in Mozilla Firefox before 18.0, Firefox ESR 17.x before 17.0.2, Thunderbird before 17.0.2, Thunderbird ESR 17.x before 17.0.2, and SeaMonkey before 2.15 does not prevent modifications to the prototype of an object, which allows remote attackers to execute arbitrary JavaScript code with chrome privileges by referencing Object.prototype.__proto__ in a crafted HTML document.
CVE-2008-5052	The AppendAttributeValue function in the JavaScript engine in Mozilla Firefox 2.x before 2.0.0.18, Thunderbird 2.x before 2.0.0.18, and SeaMonkey 1.x before 1.1.13 allows remote attackers to cause a denial of service (crash) via unknown vectors that trigger memory corruption, as demonstrated by e4x/extensions/regress-410192.js.
CVE-2013-5590	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 25.0, Firefox ESR 17.x before 17.0.10 and 24.x before 24.1, Thunderbird before 24.1, Thunderbird ESR 17.x before 17.0.10, and SeaMonkey before 2.22 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2012-0463	The nsWindow implementation in the browser engine in Mozilla Firefox before 3.6.28 and 4.x through 10.0, Firefox ESR 10.x before 10.0.3, Thunderbird before 3.1.20 and 5.0 through 10.0, Thunderbird ESR 10.x before 10.0.3, and SeaMonkey before 2.8 does not check the validity of an instance after event dispatching, which allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors, as demonstrated by Mobile Firefox on Android.
CVE-2007-3845	Mozilla Firefox before 2.0.0.6, Thunderbird before 1.5.0.13 and 2.x before 2.0.0.6, and SeaMonkey before 1.1.4 allow remote attackers to execute arbitrary commands via certain vectors associated with launching "a file handling program based on the file extension at the end of the URI," a variant of CVE-2007-4041. NOTE: the vendor states that "it is still possible to launch a filetype handler based on extension rather than the registered protocol handler."
CVE-2002-1121	SMTP content filter engines, including (1) GFI MailSecurity for Exchange/SMTP before 7.2, (2) InterScan VirusWall before 3.52 build 1494, (3) the default configuration of MIMEDefang before 2.21, and possibly other products, do not detect fragmented emails as defined in RFC2046 ("Message Fragmentation and Reassembly") and supported in such products as Outlook Express, which allows remote attackers to bypass content filtering, including virus checking, via fragmented emails of the message/partial content type.
CVE-2010-2754	dom/base/nsJSEnvironment.cpp in Mozilla Firefox 3.5.x before 3.5.11 and 3.6.x before 3.6.7, Thunderbird 3.0.x before 3.0.6 and 3.1.x before 3.1.1, and SeaMonkey before 2.0.6 does not properly suppress a script's URL in certain circumstances involving a redirect and an error message, which allows remote attackers to obtain sensitive information about script parameters via a crafted HTML document, related to the window.onerror handler.
CVE-2011-2983	Mozilla Firefox before 3.6.20, Thunderbird 2.x and 3.x before 3.1.12, SeaMonkey 1.x and 2.x, and possibly other products does not properly handle the RegExp.input property, which allows remote attackers to bypass the Same Origin Policy and read data from a different domain via a crafted web site, possibly related to a use-after-free.
CVE-2011-3648	Cross-site scripting (XSS) vulnerability in Mozilla Firefox before 3.6.24 and 4.x through 7.0 and Thunderbird before 3.1.6 and 5.0 through 7.0 allows remote attackers to inject arbitrary web script or HTML via crafted text with Shift JIS encoding.
CVE-2014-1479	The System Only Wrapper (SOW) implementation in Mozilla Firefox before 27.0, Firefox ESR 24.x before 24.3, Thunderbird before 24.3, and SeaMonkey before 2.24 does not prevent certain cloning operations, which allows remote attackers to bypass intended restrictions on XUL content via vectors involving XBL content scopes.
CVE-2012-1957	An unspecified parser-utility class in Mozilla Firefox 4.x through 13.0, Firefox ESR 10.x before 10.0.6, Thunderbird 5.0 through 13.0, Thunderbird ESR 10.x before 10.0.6, and SeaMonkey before 2.11 does not properly handle EMBED elements within description elements in RSS feeds, which allows remote attackers to conduct cross-site scripting (XSS) attacks via a feed.
CVE-2012-1945	Mozilla Firefox 4.x through 12.0, Firefox ESR 10.x before 10.0.5, Thunderbird 5.0 through 12.0, Thunderbird ESR 10.x before 10.0.5, and SeaMonkey before 2.10 allow local users to obtain sensitive information via an HTML document that loads a shortcut (aka .lnk) file for display within an IFRAME element, as demonstrated by a network share implemented by (1) Microsoft Windows or (2) Samba.
CVE-2008-5512	Multiple unspecified vulnerabilities in Mozilla Firefox 3.x before 3.0.5 and 2.x before 2.0.0.19, Thunderbird 2.x before 2.0.0.19, and SeaMonkey 1.x before 1.1.14 allow remote attackers to run arbitrary JavaScript with chrome privileges via unknown vectors in which "page content can pollute XPCNativeWrappers."
CVE-2012-4191	The mozilla::net::FailDelayManager::Lookup function in the WebSockets implementation in Mozilla Firefox before 16.0.1, Thunderbird before 16.0.1, and SeaMonkey before 2.13.1 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unspecified vectors.
CVE-2015-2710	Heap-based buffer overflow in the SVGTextFrame class in Mozilla Firefox before 38.0, Firefox ESR 31.x before 31.7, and Thunderbird before 31.7 allows remote attackers to execute arbitrary code via crafted SVG graphics data in conjunction with a crafted Cascading Style Sheets (CSS) token sequence.
CVE-2015-2740	Buffer overflow in the nsXMLHttpRequest::AppendToResponseText function in Mozilla Firefox before 39.0, Firefox ESR 31.x before 31.8 and 38.x before 38.1, and Thunderbird before 38.1 might allow remote attackers to cause a denial of service or have unspecified other impact via unknown vectors.
CVE-2008-5430	Mozilla Thunderbird 2.0.14 does not properly handle (1) multipart/mixed e-mail messages with many MIME parts and possibly (2) e-mail messages with many "Content-type: message/rfc822;" headers, which might allow remote attackers to cause a denial of service (stack consumption or other resource consumption) via a large e-mail message, a related issue to CVE-2006-1173.
CVE-2013-5599	Use-after-free vulnerability in the nsIPresShell::GetPresContext function in the PresShell (aka presentation shell) implementation in Mozilla Firefox before 25.0, Firefox ESR 17.x before 17.0.10 and 24.x before 24.1, Thunderbird before 24.1, Thunderbird ESR 17.x before 17.0.10, and SeaMonkey before 2.22 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption and application crash) via vectors involving a CANVAS element, a mozTextStyle attribute, and an onresize event.
CVE-2007-5340	Multiple vulnerabilities in the Javascript engine in Mozilla Firefox before 2.0.0.8, Thunderbird before 2.0.0.8, and SeaMonkey before 1.1.5 allow remote attackers to cause a denial of service (crash) via crafted HTML that triggers memory corruption.

CVE-2008-0420	modules/libpr0n/decoders/bmp/nsBMPDecoder.cpp in Mozilla Firefox before 2.0.0.12, Thunderbird before 2.0.0.12, and SeaMonkey before 1.1.8 does not properly perform certain calculations related to the mColors table, which allows remote attackers to read portions of memory uninitialized via a crafted 8-bit bitmap (BMP) file that triggers an out-of-bounds read within the heap, as demonstrated using a CANVAS element; or cause a denial of service (application crash) via a crafted 8-bit bitmap file that triggers an out-of-bounds read. NOTE: the initial public reports stated that this affected Firefox in Ubuntu 6.06 through 7.10.
CVE-2012-5842	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0, Thunderbird ESR 10.x before 10.0.11, and SeaMonkey before 2.14 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2013-1738	Use-after-free vulnerability in the JS_GetGlobalForScopeChain function in Mozilla Firefox before 24.0, Thunderbird before 24.0, and SeaMonkey before 2.21 allows remote attackers to execute arbitrary code by leveraging incorrect garbage collection in situations involving default compartments and frame-chain restoration.
CVE-2009-3032	Integer overflow in kvolefio.dll 8.5.0.8339 and 10.5.0.0 in the Autonomy KeyView Filter SDK, as used in IBM Lotus Notes 8.5, Symantec Mail Security for Microsoft Exchange 5.0.10 through 5.0.13, and other products, allows context-dependent attackers to execute arbitrary code via a crafted OLE document that triggers a heap-based buffer overflow.
CVE-2012-0462	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 4.x through 10.0, Firefox ESR 10.x before 10.0.3, Thunderbird 5.0 through 10.0, Thunderbird ESR 10.x before 10.0.3, and SeaMonkey before 2.8 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2012-3972	The format-number functionality in the XSLT implementation in Mozilla Firefox before 15.0, Firefox ESR 10.x before 10.0.7, Thunderbird before 15.0, Thunderbird ESR 10.x before 10.0.7, and SeaMonkey before 2.12 allows remote attackers to obtain sensitive information via unspecified vectors that trigger a heap-based buffer over-read.
CVE-2012-0469	Use-after-free vulnerability in the mozilla::dom::indexedDB::IDBKeyRange::cycleCollection::Trace function in Mozilla Firefox 4.x through 11.0, Firefox ESR 10.x before 10.0.4, Thunderbird 5.0 through 11.0, Thunderbird ESR 10.x before 10.0.4, and SeaMonkey before 2.9 allows remote attackers to execute arbitrary code via vectors related to crafted IndexedDB data.
CVE-2008-5511	Mozilla Firefox 3.x before 3.0.5 and 2.x before 2.0.0.19, Thunderbird 2.x before 2.0.0.19, and SeaMonkey 1.x before 1.1.14 allows remote attackers to bypass the same origin policy and conduct cross-site scripting (XSS) attacks via an XBL binding to an "unloaded document."
CVE-2006-0294	Mozilla Firefox before 1.5.0.1, Thunderbird 1.5 if running Javascript in mail, and SeaMonkey before 1.0 allow remote attackers to execute arbitrary code by changing an element's style from position:relative to position:static, which causes Gecko to operate on freed memory.
CVE-2006-1045	The HTML rendering engine in Mozilla Thunderbird 1.5, when "Block loading of remote images in mail messages" is enabled, does not properly block external images from inline HTML attachments, which could allow remote attackers to obtain sensitive information, such as application version or IP address, when the user reads the email and the external image is accessed.
CVE-2008-0418	Directory traversal vulnerability in Mozilla Firefox before 2.0.0.12, Thunderbird before 2.0.0.12, and SeaMonkey before 1.1.8, when using "flat" addons, allows remote attackers to read arbitrary Javascript, image, and stylesheet files via the chrome: URI scheme, as demonstrated by stealing session information from sessionstore.js.
CVE-2012-1973	Use-after-free vulnerability in the nsObjectLoadingContent::LoadObject function in Mozilla Firefox before 15.0, Firefox ESR 10.x before 10.0.7, Thunderbird before 15.0, Thunderbird ESR 10.x before 10.0.7, and SeaMonkey before 2.12 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2014-1512	Use-after-free vulnerability in the TypeObject class in the JavaScript engine in Mozilla Firefox before 28.0, Firefox ESR 24.x before 24.4, Thunderbird before 24.4, and SeaMonkey before 2.25 allows remote attackers to execute arbitrary code by triggering extensive memory consumption while garbage collection is occurring, as demonstrated by improper handling of BumpChunk objects.
CVE-2013-5600	Use-after-free vulnerability in the nsIOService::NewChannelFromURIWithProxyFlags function in Mozilla Firefox before 25.0, Firefox ESR 17.x before 17.0.10 and 24.x before 24.1, Thunderbird before 24.1, Thunderbird ESR 17.x before 17.0.10, and SeaMonkey before 2.22 allows remote attackers to execute arbitrary code via vectors involving a blob: URL.
CVE-2015-0807	The navigator.sendBeacon implementation in Mozilla Firefox before 37.0, Firefox ESR 31.x before 31.6, and Thunderbird before 31.6 processes HTTP 30x status codes for redirects after a preflight request has occurred, which allows remote attackers to bypass intended CORS access-control checks and conduct cross-site request forgery (CSRF) attacks via a crafted web site, a similar issue to CVE-2014-8638.
CVE-2011-3663	Mozilla Firefox 4.x through 8.0, Thunderbird 5.0 through 8.0, and SeaMonkey before 2.6 allow remote attackers to capture keystrokes entered on a web page, even when JavaScript is disabled, by using SVG animation accessKey events within that web page.
CVE-2012-3986	Mozilla Firefox before 16.0, Firefox ESR 10.x before 10.0.8, Thunderbird before 16.0, Thunderbird ESR 10.x before 10.0.8, and SeaMonkey before 2.13 do not properly restrict calls to DOMWindowUtils (aka nsDOMWindowUtils) methods, which allows remote attackers to bypass intended access restrictions via crafted JavaScript code.
CVE-2012-1958	Use-after-free vulnerability in the nsGlobalWindow::PageHidden function in Mozilla Firefox 4.x through 13.0, Firefox ESR 10.x before 10.0.6, Thunderbird 5.0 through 13.0, Thunderbird ESR 10.x before 10.0.6, and SeaMonkey before 2.11 might allow remote attackers to execute arbitrary code via vectors related to focused content.
CVE-2006-2776	Certain privileged UI code in Mozilla Firefox and Thunderbird before 1.5.0.4 calls content-defined setters on an object prototype, which allows remote attackers to execute code at a higher privilege than intended.
CVE-2012-5841	Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0, Thunderbird ESR 10.x before 10.0.11, and SeaMonkey before 2.14 implement cross-origin wrappers with a filtering behavior that does not properly restrict write actions, which allows remote attackers to conduct cross-site scripting (XSS) attacks via a crafted web site.
CVE-	GUI display truncation vulnerability in Mozilla Thunderbird 1.0.2, 1.0.6, and 1.0.7 allows user-assisted attackers to execute arbitrary

2006-0236	code via an attachment with a filename containing a large number of spaces ending with a dangerous extension that is not displayed by Thunderbird, along with an inconsistent Content-Type header, which could be used to trick a user into downloading dangerous content by dragging or saving the attachment.
CVE-2014-1585	The WebRTC video-sharing feature in dom/media/MediaManager.cpp in Mozilla Firefox before 33.0, Firefox ESR 31.x before 31.2, and Thunderbird 31.x before 31.2 does not properly recognize Stop Sharing actions for videos in IFRAME elements, which allows remote attackers to obtain sensitive information from the local camera by maintaining a session after the user tries to discontinue streaming.
CVE-2012-1944	The Content Security Policy (CSP) implementation in Mozilla Firefox 4.x through 12.0, Firefox ESR 10.x before 10.0.5, Thunderbird 5.0 through 12.0, Thunderbird ESR 10.x before 10.0.5, and SeaMonkey before 2.10 does not block inline event handlers, which makes it easier for remote attackers to conduct cross-site scripting (XSS) attacks via a crafted HTML document.
CVE-2010-3179	Stack-based buffer overflow in the text-rendering functionality in Mozilla Firefox before 3.5.14 and 3.6.x before 3.6.11, Thunderbird before 3.0.9 and 3.1.x before 3.1.5, and SeaMonkey before 2.0.9 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a long argument to the document.write method.
CVE-2011-2372	Mozilla Firefox before 3.6.23 and 4.x through 6, Thunderbird before 7.0, and SeaMonkey before 2.4 do not prevent the starting of a download in response to the holding of the Enter key, which allows user-assisted remote attackers to bypass intended access restrictions via a crafted web site.
CVE-2015-2708	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 38.0, Firefox ESR 31.x before 31.7, and Thunderbird before 31.7 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2014-1511	Mozilla Firefox before 28.0, Firefox ESR 24.x before 24.4, Thunderbird before 24.4, and SeaMonkey before 2.25 allow remote attackers to bypass the popup blocker via unspecified vectors.
CVE-2009-2404	Heap-based buffer overflow in a regular-expression parser in Mozilla Network Security Services (NSS) before 3.12.3, as used in Firefox, Thunderbird, SeaMonkey, Evolution, Pidgin, and AOL Instant Messenger (AIM), allows remote SSL servers to cause a denial of service (application crash) or possibly execute arbitrary code via a long domain name in the subject's Common Name (CN) field of an X.509 certificate, related to the cert_TestHostName function.
CVE-2013-5601	Use-after-free vulnerability in the nsEventListenerManager::SetEventHandler function in Mozilla Firefox before 25.0, Firefox ESR 17.x before 17.0.10 and 24.x before 24.1, Thunderbird before 24.1, Thunderbird ESR 17.x before 17.0.10, and SeaMonkey before 2.22 allows remote attackers to execute arbitrary code via vectors related to a memory allocation through the garbage collection (GC) API.
CVE-2013-0764	The nsSOCKSSocketInfo::ConnectToProxy function in Mozilla Firefox before 18.0, Firefox ESR 17.x before 17.0.2, Thunderbird before 17.0.2, Thunderbird ESR 17.x before 17.0.2, and SeaMonkey before 2.15 does not ensure thread safety for SSL sessions, which allows remote attackers to execute arbitrary code via crafted data, as demonstrated by e-mail message data.
CVE-2013-1684	Use-after-free vulnerability in the mozilla::dom::HTMLMediaElement::LookupMediaElementURITable function in Mozilla Firefox before 22.0, Firefox ESR 17.x before 17.0.7, Thunderbird before 17.0.7, and Thunderbird ESR 17.x before 17.0.7 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via a crafted web site.
CVE-2011-2984	Mozilla Firefox before 3.6.20, SeaMonkey 2.x, Thunderbird 3.x before 3.1.12, and possibly other products does not properly handle the dropping of a tab element, which allows remote attackers to execute arbitrary JavaScript code with chrome privileges by establishing a content area and registering for drop events.
CVE-2013-5602	The Worker::SetEventListener function in the Web workers implementation in Mozilla Firefox before 25.0, Firefox ESR 17.x before 17.0.10 and 24.x before 24.1, Thunderbird before 24.1, Thunderbird ESR 17.x before 17.0.10, and SeaMonkey before 2.22 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via vectors related to direct proxies.
CVE-2010-0174	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 3.0.19, 3.5.x before 3.5.9, and 3.6.x before 3.6.2; Thunderbird before 3.0.4; and SeaMonkey before 2.0.4 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2013-0765	Mozilla Firefox before 19.0, Thunderbird before 17.0.3, and SeaMonkey before 2.16 do not prevent multiple wrapping of WebIDL objects, which allows remote attackers to bypass intended access restrictions via unspecified vectors.
CVE-2004-0423	The log_event function in ssmtp 2.50.6 and earlier allows local users to overwrite arbitrary files via a symlink attack on the ssmtp.log temporary log file.
CVE-2012-0461	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 3.6.28 and 4.x through 10.0, Firefox ESR 10.x before 10.0.3, Thunderbird before 3.1.20 and 5.0 through 10.0, Thunderbird ESR 10.x before 10.0.3, and SeaMonkey before 2.8 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2011-0061	Buffer overflow in Mozilla Firefox 3.6.x before 3.6.14, Thunderbird before 3.1.8, and SeaMonkey before 2.0.12 might allow remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted JPEG image.
CVE-2012-3974	Untrusted search path vulnerability in the installer in Mozilla Firefox before 15.0, Firefox ESR 10.x before 10.0.7, Thunderbird before 15.0, and Thunderbird ESR 10.x before 10.0.7 on Windows allows local users to gain privileges via a Trojan horse executable file in a root directory.
CVE-2006-5487	Directory traversal vulnerability in Marshal MailMarshal SMTP 5.x, 6.x, and 2006, and MailMarshal for Exchange 5.x, allows remote attackers to write arbitrary files via ".." sequences in filenames in an ARJ compressed archive.
CVE-2008-5508	Mozilla Firefox 3.x before 3.0.5 and 2.x before 2.0.0.19, Thunderbird 2.x before 2.0.0.19, and SeaMonkey 1.x before 1.1.14 does not properly parse URLs with leading whitespace or control characters, which might allow remote attackers to misrepresent URLs and simplify phishing attacks.

CVE-2006-5748	Multiple unspecified vulnerabilities in the JavaScript engine in Mozilla Firefox before 1.5.0.8, Thunderbird before 1.5.0.8, and SeaMonkey before 1.0.6 allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via unspecified vectors that trigger memory corruption.
CVE-2013-0766	Use-after-free vulnerability in the ~nsHTMLEditRules implementation in Mozilla Firefox before 18.0, Firefox ESR 10.x before 10.0.12 and 17.x before 17.0.1, Thunderbird before 17.0.2, Thunderbird ESR 10.x before 10.0.12 and 17.x before 17.0.1, and SeaMonkey before 2.15 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2013-1736	The nsGfxScrollFrameInner::IsLTR function in Mozilla Firefox before 24.0, Firefox ESR 17.x before 17.0.9, Thunderbird before 24.0, Thunderbird ESR 17.x before 17.0.9, and SeaMonkey before 2.21 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via vectors related to improperly establishing parent-child relationships of range-request nodes.
CVE-2013-5595	The JavaScript engine in Mozilla Firefox before 25.0, Firefox ESR 17.x before 17.0.10 and 24.x before 24.1, Thunderbird before 24.1, Thunderbird ESR 17.x before 17.0.10, and SeaMonkey before 2.22 does not properly allocate memory for unspecified functions, which allows remote attackers to conduct buffer overflow attacks via a crafted web page.
CVE-2010-0161	The nsAuthSSPI::Unwrap function in extensions/auth/nsAuthSSPI.cpp in Mozilla Thunderbird before 2.0.0.24 and SeaMonkey before 1.1.19 on Windows Vista, Windows Server 2008 R2, and Windows 7 allows remote SMTP, IMAP, and POP servers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via crafted data in a session that uses SSPI.
CVE-2011-2985	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 4.x through 5, Thunderbird before 6, SeaMonkey 2.x before 2.3, and possibly other products allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2013-0800	Integer signedness error in the pixman_fill_sse2 function in pixman-sse2.c in Pixman, as distributed with Cairo and used in Mozilla Firefox before 20.0, Firefox ESR 17.x before 17.0.5, Thunderbird before 17.0.5, Thunderbird ESR 17.x before 17.0.5, SeaMonkey before 2.17, and other products, allows remote attackers to execute arbitrary code via crafted values that trigger attempted use of a (1) negative box boundary or (2) negative box size, leading to an out-of-bounds write operation.
CVE-2008-7258	** DISPUTED ** The standardise function in Anibal Monsalve Salazar sSMTP 2.61 and 2.62 allows local users to cause a denial of service (application exit) via an e-mail message containing a long line that begins with a . (dot) character. NOTE: CVE disputes this issue because it is solely a usability problem for senders of messages with certain long lines, and has no security impact.
CVE-2011-3661	YARR, as used in Mozilla Firefox 4.x through 8.0, Thunderbird 5.0 through 8.0, and SeaMonkey before 2.6, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via crafted JavaScript.
CVE-2011-3649	Mozilla Firefox 7.0 and Thunderbird 7.0, when the Direct2D (aka D2D) API is used on Windows in conjunction with the Azure graphics back-end, allow remote attackers to bypass the Same Origin Policy, and obtain sensitive image data from a different domain, by inserting this data into a canvas. NOTE: this issue exists because of a CVE-2011-2986 regression.
CVE-2006-3807	Mozilla Firefox before 1.5.0.5, Thunderbird before 1.5.0.5, and SeaMonkey before 1.0.3 allows remote attackers to execute arbitrary code via script that changes the standard Object() constructor to return a reference to a privileged object and calling "named JavaScript functions" that use the constructor.
CVE-2013-5613	Use-after-free vulnerability in the PresShell::DispatchSynthMouseMove function in Mozilla Firefox before 26.0, Firefox ESR 24.x before 24.2, Thunderbird before 24.2, and SeaMonkey before 2.23 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via vectors involving synthetic mouse movement, related to the RestyleManager::GetHoverGeneration function.
CVE-2011-3659	Use-after-free vulnerability in Mozilla Firefox before 3.6.26 and 4.x through 9.0, Thunderbird before 3.1.18 and 5.0 through 9.0, and SeaMonkey before 2.7 might allow remote attackers to execute arbitrary code via vectors related to incorrect AttributeChildRemoved notifications that affect access to removed nsDOMAttribute child nodes.
CVE-2008-5507	Mozilla Firefox 3.x before 3.0.5 and 2.x before 2.0.0.19, Thunderbird 2.x before 2.0.0.19, and SeaMonkey 1.x before 1.1.14 allow remote attackers to bypass the same origin policy and access portions of data from another domain via a JavaScript URL that redirects to the target resource, which generates an error if the target data does not have JavaScript syntax, which can be accessed using the window.onerror DOM API.
CVE-2011-0062	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 3.6.x before 3.6.14 and Thunderbird 3.1.x before 3.1.8 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2012-4196	Mozilla Firefox before 16.0.2, Firefox ESR 10.x before 10.0.10, Thunderbird before 16.0.2, Thunderbird ESR 10.x before 10.0.10, and SeaMonkey before 2.13.2 allow remote attackers to bypass the Same Origin Policy and read the Location object via a prototype property-injection attack that defeats certain protection mechanisms for this object.
CVE-2012-1947	Heap-based buffer overflow in the utf16_to_isolatin1 function in Mozilla Firefox 4.x through 12.0, Firefox ESR 10.x before 10.0.5, Thunderbird 5.0 through 12.0, Thunderbird ESR 10.x before 10.0.5, and SeaMonkey before 2.10 allows remote attackers to execute arbitrary code via vectors that trigger a character-set conversion failure.
CVE-2006-1738	Unspecified vulnerability in Mozilla Firefox and Thunderbird 1.x before 1.5 and 1.0.x before 1.0.8, Mozilla Suite before 1.7.13, and SeaMonkey before 1.0 allows remote attackers to cause a denial of service (crash) by changing the (1) -moz-grid and (2) -moz-grid-group display styles.
CVE-2005-2261	Firefox before 1.0.5, Thunderbird before 1.0.5, Mozilla before 1.7.9, Netscape 8.0.2, and K-Meleon 0.9 runs XBL scripts even when Javascript has been disabled, which makes it easier for remote attackers to bypass such protection.
CVE-2012-5843	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 17.0, Thunderbird before 17.0, and SeaMonkey before 2.14 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2014-	vmtypedarrayobject.cpp in Mozilla Firefox before 28.0, Firefox ESR 24.x before 24.4, Thunderbird before 24.4, and SeaMonkey before 2.25 does not validate the length of the destination array before a copy operation, which allows remote attackers to execute arbitrary

1514	code or cause a denial of service (out-of-bounds write and application crash) by triggering incorrect use of the TypedArrayObject class.
CVE-2012-4204	The str_unescape function in the JavaScript engine in Mozilla Firefox before 17.0, Thunderbird before 17.0, and SeaMonkey before 2.14 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via unspecified vectors.
CVE-2013-5596	The cycle collection (CC) implementation in Mozilla Firefox before 25.0, Firefox ESR 24.x before 24.1, Thunderbird before 24.1, and SeaMonkey before 2.22 does not properly determine the thread for release of an image object, which allows remote attackers to execute arbitrary code or cause a denial of service (race condition and application crash) via a large HTML document containing IMG elements, as demonstrated by the Never-Ending Reddit on reddit.com.
CVE-2013-0799	Buffer overflow in the Mozilla Maintenance Service in Mozilla Firefox before 20.0, Firefox ESR 17.x before 17.0.5, Thunderbird before 17.0.5, and Thunderbird ESR 17.x before 17.0.5 on Windows allows local users to gain privileges via crafted arguments.
CVE-2013-0767	The nsSVGPathElement::GetPathLengthScale function in Mozilla Firefox before 18.0, Firefox ESR 10.x before 10.0.12 and 17.x before 17.0.1, Thunderbird before 17.0.2, Thunderbird ESR 10.x before 10.0.12 and 17.x before 17.0.1, and SeaMonkey before 2.15 allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2015-2735	nsZipArchive.cpp in Mozilla Firefox before 39.0, Firefox ESR 31.x before 31.8 and 38.x before 38.1, and Thunderbird before 38.1 accesses unintended memory locations, which allows remote attackers to have an unspecified impact via a crafted ZIP archive.
CVE-2008-5510	The CSS parser in Mozilla Firefox 3.x before 3.0.5 and 2.x before 2.0.0.19, Thunderbird 2.x before 2.0.0.19, and SeaMonkey 1.x before 1.1.14 ignores the '\0' escaped null character, which might allow remote attackers to bypass protection mechanisms such as sanitization routines.
CVE-2012-0468	The browser engine in Mozilla Firefox 4.x through 11.0, Thunderbird 5.0 through 11.0, and SeaMonkey before 2.9 allows remote attackers to cause a denial of service (assertion failure and memory corruption) or possibly execute arbitrary code via vectors related to jsval.h and the js::array_shift function.
CVE-2013-5597	Use-after-free vulnerability in the nsDocLoader::doStopDocumentLoad function in Mozilla Firefox before 25.0, Firefox ESR 17.x before 17.0.10 and 24.x before 24.1, Thunderbird before 24.1, Thunderbird ESR 17.x before 17.0.10, and SeaMonkey before 2.22 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via vectors involving a state-change event during an update of the offline cache.
CVE-2012-5354	Mozilla Firefox before 16.0, Thunderbird before 16.0, and SeaMonkey before 2.13 do not properly handle navigation away from a web page that has multiple menus of SELECT elements active, which allows remote attackers to conduct clickjacking attacks via vectors involving an XPI file, the window.open method, and the Geolocation API, a different vulnerability than CVE-2012-3984.
CVE-2012-1974	Use-after-free vulnerability in the gfxTextRun::CanBreakLineBefore function in Mozilla Firefox before 15.0, Firefox ESR 10.x before 10.0.7, Thunderbird before 15.0, Thunderbird ESR 10.x before 10.0.7, and SeaMonkey before 2.12 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2009-3037	Buffer overflow in xlssr.dll in the Autonomy KeyView XLS viewer (aka File Viewer for Excel), as used in IBM Lotus Notes 5.x through 8.5.x, Symantec Mail Security, Symantec BrightMail Appliance, Symantec Data Loss Prevention (DLP), and other products, allows remote attackers to execute arbitrary code via a crafted .xls spreadsheet attachment.
CVE-2013-1737	Mozilla Firefox before 24.0, Firefox ESR 17.x before 17.0.9, Thunderbird before 24.0, Thunderbird ESR 17.x before 17.0.9, and SeaMonkey before 2.21 do not properly identify the "this" object during use of user-defined getter methods on DOM proxies, which might allow remote attackers to bypass intended access restrictions via vectors involving an expando object.
CVE-2014-1586	content/base/src/nsDocument.cpp in Mozilla Firefox before 33.0, Firefox ESR 31.x before 31.2, and Thunderbird 31.x before 31.2 does not consider whether WebRTC video sharing is occurring, which allows remote attackers to obtain sensitive information from the local camera in certain IFRAME situations by maintaining a session after the user temporarily navigates away.
CVE-2012-1959	Mozilla Firefox 4.x through 13.0, Firefox ESR 10.x before 10.0.6, Thunderbird 5.0 through 13.0, Thunderbird ESR 10.x before 10.0.6, and SeaMonkey before 2.11 do not consider the presence of same-compartment security wrappers (SCSW) during the cross-compartment wrapping of objects, which allows remote attackers to bypass intended XBL access restrictions via crafted content.
CVE-2012-0460	Mozilla Firefox 4.x through 10.0, Firefox ESR 10.x before 10.0.3, Thunderbird 5.0 through 10.0, Thunderbird ESR 10.x before 10.0.3, and SeaMonkey before 2.8 do not properly restrict write access to the window.fullScreen object, which allows remote attackers to spoof the user interface via a crafted web page.
CVE-2014-2018	Cross-site scripting (XSS) vulnerability in Mozilla Thunderbird 17.x through 17.0.8, Thunderbird ESR 17.x through 17.0.10, and SeaMonkey before 2.20 allows user-assisted remote attackers to inject arbitrary web script or HTML via an e-mail message containing a data: URL in a (1) OBJECT or (2) EMBED element, a related issue to CVE-2013-6674.
CVE-2012-3985	Mozilla Firefox before 16.0, Thunderbird before 16.0, and SeaMonkey before 2.13 do not properly implement the HTML5 Same Origin Policy, which allows remote attackers to conduct cross-site scripting (XSS) attacks by leveraging initial-origin access after document.domain has been set.
CVE-2012-4192	Mozilla Firefox 16.0, Thunderbird 16.0, and SeaMonkey 2.13 allow remote attackers to bypass the Same Origin Policy and read the properties of a Location object via a crafted web site, a related issue to CVE-2012-4193.
CVE-2012-1946	Use-after-free vulnerability in the nsINode::ReplaceOrInsertBefore function in Mozilla Firefox 4.x through 12.0, Firefox ESR 10.x before 10.0.5, Thunderbird 5.0 through 12.0, Thunderbird ESR 10.x before 10.0.5, and SeaMonkey before 2.10 might allow remote attackers to execute arbitrary code via document changes involving replacement or insertion of a node.
CVE-2010-0175	Use-after-free vulnerability in the nsTreeSelection implementation in Mozilla Firefox before 3.0.19 and 3.5.x before 3.5.9, Thunderbird before 3.0.4, and SeaMonkey before 2.0.4 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via unspecified vectors that trigger a call to the handler for the select event for XUL tree items.
CVE-2014-	Use-after-free vulnerability in the RefreshDriverTimer::TickDriver function in the SMIL Animation Controller in Mozilla Firefox before 30.0, Firefox ESR 24.x before 24.6, and Thunderbird before 24.6 allows remote attackers to execute arbitrary code or cause a denial of

1541	service (heap memory corruption) via crafted web content.
CVE-2006-6504	Mozilla Firefox 2.x before 2.0.0.1, 1.5.x before 1.5.0.9, and SeaMonkey before 1.0.7 allows remote attackers to execute arbitrary code by appending an SVG comment DOM node to another type of document, which triggers memory corruption.
CVE-2005-2387	Multiple stack-based buffer overflows in GoodTech SMTP server 5.16 allow remote attackers to execute arbitrary code via (1) a RCPT TO command with a long DNS name, or (2) a large number of RCPT TO commands with a long e-mail name arugment in the last command.
CVE-2011-2995	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 3.6.23 and 4.x through 6, Thunderbird before 7.0, and SeaMonkey before 2.4 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2014-1513	TypedArrayObject.cpp in Mozilla Firefox before 28.0, Firefox ESR 24.x before 24.4, Thunderbird before 24.4, and SeaMonkey before 2.25 does not prevent a zero-length transition during use of an ArrayBuffer object, which allows remote attackers to execute arbitrary code or cause a denial of service (heap-based out-of-bounds write or read) via a crafted web site.
CVE-2010-3765	Mozilla Firefox 3.5.x through 3.5.14 and 3.6.x through 3.6.11, Thunderbird 3.1.6 before 3.1.6 and 3.0.x before 3.0.10, and SeaMonkey 2.x before 2.0.10, when JavaScript is enabled, allows remote attackers to execute arbitrary code via vectors related to nsCSSFrameConstructor::ContentAppended, the appendChild method, incorrect index tracking, and the creation of multiple frames, which triggers memory corruption, as exploited in the wild in October 2010 by the Belmoo malware.
CVE-2013-1682	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 22.0, Firefox ESR 17.x before 17.0.7, Thunderbird before 17.0.7, and Thunderbird ESR 17.x before 17.0.7 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2011-2986	Mozilla Firefox 4.x through 5, Thunderbird before 6, SeaMonkey 2.x before 2.3, and possibly other products, when the Direct2D (aka D2D) API is used on Windows, allows remote attackers to bypass the Same Origin Policy, and obtain sensitive image data from a different domain, by inserting this data into a canvas.
CVE-2013-0797	Untrusted search path vulnerability in the Mozilla Updater in Mozilla Firefox before 20.0, Firefox ESR 17.x before 17.0.5, Thunderbird before 17.0.5, Thunderbird ESR 17.x before 17.0.5, and SeaMonkey before 2.17 allows local users to gain privileges via a Trojan horse DLL file in an unspecified directory.
CVE-2013-5615	The JavaScript implementation in Mozilla Firefox before 26.0, Firefox ESR 24.x before 24.2, Thunderbird before 24.2, and SeaMonkey before 2.23 does not properly enforce certain typeset restrictions on the generation of GetElementIC typed array stubs, which has unspecified impact and remote attack vectors.
CVE-2013-1690	Mozilla Firefox before 22.0, Firefox ESR 17.x before 17.0.7, Thunderbird before 17.0.7, and Thunderbird ESR 17.x before 17.0.7 do not properly handle onreadystatechange events in conjunction with page reloading, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted web site that triggers an attempt to execute data at an unmapped memory location.
CVE-2012-1976	Use-after-free vulnerability in the nsHTMLSelectElement::SubmitNamesValues function in Mozilla Firefox before 15.0, Firefox ESR 10.x before 10.0.7, Thunderbird before 15.0, Thunderbird ESR 10.x before 10.0.7, and SeaMonkey before 2.12 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2012-4195	The nsLocation::CheckURL function in Mozilla Firefox before 16.0.2, Firefox ESR 10.x before 10.0.10, Thunderbird before 16.0.2, Thunderbird ESR 10.x before 10.0.10, and SeaMonkey before 2.13.2 does not properly determine the calling document and principal in its return value, which makes it easier for remote attackers to conduct cross-site scripting (XSS) attacks via a crafted web site, and makes it easier for remote attackers to execute arbitrary JavaScript code by leveraging certain add-on behavior.
CVE-2016-1966	The nsNPObjWrapper::GetNewOrUsed function in dom/plugins/base/nsJSNPRuntime.cpp in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7 allows remote attackers to execute arbitrary code or cause a denial of service (invalid pointer dereference and memory corruption) via a crafted NPAPI plugin.
CVE-2000-1130	McAfee WebShield SMTP 4.5 allows remote attackers to bypass email content filtering rules by including Extended ASCII characters in name of the attachment.
CVE-2014-1539	Mozilla Firefox before 30.0 and Thunderbird through 24.6 on OS X do not ensure visibility of the cursor after interaction with a Flash object and a DIV element, which makes it easier for remote attackers to conduct clickjacking attacks via JavaScript code that produces a fake cursor image.
CVE-2005-3027	Sybari Antigen 8.0 SR2 does not properly filter SMTP messages, which allows remote attackers to bypass custom filter rules and send file attachments of arbitrary file types via a message with a subject of "Antigen forwarded attachment".
CVE-2010-3180	Use-after-free vulnerability in the nsBarProp function in Mozilla Firefox before 3.5.14 and 3.6.x before 3.6.11, Thunderbird before 3.0.9 and 3.1.x before 3.1.5, and SeaMonkey before 2.0.9 allows remote attackers to execute arbitrary code by accessing the locationbar property of a closed window.
CVE-2005-2602	Mozilla Thunderbird 1.0 and Firefox 1.0.6 allows remote attackers to obfuscate URIs via a long URI, which causes the address bar to go blank and could facilitate phishing attacks.
CVE-2008-0394	Buffer overflow in Citadel SMTP server 7.10 and earlier allows remote attackers to execute arbitrary code via a long RCPT TO command, which is not properly handled by the makeuserkey function. NOTE: some of these details were obtained from third party information.
CVE-2013-1692	Mozilla Firefox before 22.0, Firefox ESR 17.x before 17.0.7, Thunderbird before 17.0.7, and Thunderbird ESR 17.x before 17.0.7 do not prevent the inclusion of body data in an XMLHttpRequest HEAD request, which makes it easier for remote attackers to conduct cross-site request forgery (CSRF) attacks via a crafted web site.

CVE-2006-2786	HTTP response smuggling vulnerability in Mozilla Firefox and Thunderbird before 1.5.0.4, when used with certain proxy servers, allows remote attackers to cause Firefox to interpret certain responses as if they were responses from two different sites via (1) invalid HTTP response headers with spaces between the header name and the colon, which might not be ignored in some cases, or (2) HTTP 1.1 headers through an HTTP 1.0 proxy, which are ignored by the proxy but processed by the client.
CVE-2013-0796	The WebGL subsystem in Mozilla Firefox before 20.0, Firefox ESR 17.x before 17.0.5, Thunderbird before 17.0.5, Thunderbird ESR 17.x before 17.0.5, and SeaMonkey before 2.17 on Linux does not properly interact with Mesa drivers, which allows remote attackers to execute arbitrary code or cause a denial of service (free of unallocated memory) via unspecified vectors.
CVE-2011-3660	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 4.x through 8.0, Thunderbird 5.0 through 8.0, and SeaMonkey before 2.6 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors that trigger a compartment mismatch associated with the nsDOMMessageEvent::GetData function, and unknown other vectors.
CVE-2011-3650	Mozilla Firefox before 3.6.24 and 4.x through 7.0 and Thunderbird before 3.1.6 and 5.0 through 7.0 do not properly handle JavaScript files that contain many functions, which allows user-assisted remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via a crafted file that is accessed by debugging APIs, as demonstrated by Firebug.
CVE-2000-0932	MAILsweeper for SMTP 3.x does not properly handle corrupt CDA documents in a ZIP file and hangs, which allows remote attackers to cause a denial of service.
CVE-2011-2987	Heap-based buffer overflow in Almost Native Graphics Layer Engine (ANGLE), as used in the WebGL implementation in Mozilla Firefox 4.x through 5, Thunderbird before 6, SeaMonkey 2.x before 2.3, and possibly other products might allow remote attackers to execute arbitrary code via unspecified vectors.
CVE-2012-0459	The Cascading Style Sheets (CSS) implementation in Mozilla Firefox 4.x through 10.0, Firefox ESR 10.x before 10.0.3, Thunderbird 5.0 through 10.0, Thunderbird ESR 10.x before 10.0.3, and SeaMonkey before 2.8 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via dynamic modification of a keyframe followed by access to the cssText of the keyframe.
CVE-2012-3975	The DOMParser component in Mozilla Firefox before 15.0, Thunderbird before 15.0, and SeaMonkey before 2.12 loads subresources during parsing of text/html data within an extension, which allows remote attackers to obtain sensitive information by providing crafted data to privileged extension code.
CVE-2010-0176	Mozilla Firefox before 3.0.19, 3.5.x before 3.5.9, and 3.6.x before 3.6.2; Thunderbird before 3.0.4; and SeaMonkey before 2.0.4 do not properly manage reference counts for option elements in a XUL tree optgroup, which might allow remote attackers to execute arbitrary code via unspecified vectors that trigger access to deleted elements, related to a "dangling pointer vulnerability."
CVE-2009-3942	Martin Lambers msmtp before 1.4.19, when OpenSSL is used, does not properly handle a '\0' character in a domain name in the (1) subject's Common Name or (2) Subject Alternative Name field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.
CVE-2013-0761	Use-after-free vulnerability in the mozilla::TrackUnionStream::EndTrack implementation in Mozilla Firefox before 18.0, Firefox ESR 17.x before 17.0.1, Thunderbird before 17.0.2, Thunderbird ESR 17.x before 17.0.1, and SeaMonkey before 2.15 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2013-1693	The SVG filter implementation in Mozilla Firefox before 22.0, Firefox ESR 17.x before 17.0.7, Thunderbird before 17.0.7, and Thunderbird ESR 17.x before 17.0.7 allows remote attackers to read pixel values, and possibly bypass the Same Origin Policy and read text from a different domain, by observing timing differences in execution of filter code.
CVE-2013-0795	The System Only Wrapper (SOW) implementation in Mozilla Firefox before 20.0, Firefox ESR 17.x before 17.0.5, Thunderbird before 17.0.5, Thunderbird ESR 17.x before 17.0.5, and SeaMonkey before 2.17 does not prevent use of the cloneNode method for cloning a protected node, which allows remote attackers to bypass the Same Origin Policy or possibly execute arbitrary JavaScript code with chrome privileges via a crafted web site.
CVE-2011-0083	Use-after-free vulnerability in the nsSVGPathSegList::ReplaceItem function in the implementation of SVG element lists in Mozilla Firefox before 3.6.18, Thunderbird before 3.1.11, and SeaMonkey through 2.0.14 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via vectors involving a user-supplied callback.
CVE-2001-1456	Buffer overflow in the (1) smap/smapd and (2) CSMAP daemons for Gauntlet Firewall 5.0 through 6.0 allows remote attackers to execute arbitrary code via a crafted mail message.
CVE-2012-4188	Heap-based buffer overflow in the Convolve3x3 function in Mozilla Firefox before 16.0, Firefox ESR 10.x before 10.0.8, Thunderbird before 16.0, Thunderbird ESR 10.x before 10.0.8, and SeaMonkey before 2.13 allows remote attackers to execute arbitrary code via unspecified vectors.
CVE-2012-1953	The ElementAnimations::EnsureStyleRuleFor function in Mozilla Firefox 4.x through 13.0, Firefox ESR 10.x before 10.0.6, Thunderbird 5.0 through 13.0, Thunderbird ESR 10.x before 10.0.6, and SeaMonkey before 2.11 allows remote attackers to cause a denial of service (buffer over-read, incorrect pointer dereference, and heap-based buffer overflow) or possibly execute arbitrary code via a crafted web site.
CVE-2012-1975	Use-after-free vulnerability in the PresShell::CompleteMove function in Mozilla Firefox before 15.0, Firefox ESR 10.x before 10.0.7, Thunderbird before 15.0, Thunderbird ESR 10.x before 10.0.7, and SeaMonkey before 2.12 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2013-1694	The PreserveWrapper implementation in Mozilla Firefox before 22.0, Firefox ESR 17.x before 17.0.7, Thunderbird before 17.0.7, and Thunderbird ESR 17.x before 17.0.7 does not properly handle the lack of a wrapper, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code by leveraging unintended clearing of the wrapper cache's preserved-wrapper flag.
CVE-2011-	The SVG implementation in Mozilla Firefox 8.0, Thunderbird 8.0, and SeaMonkey 2.5 does not properly interact with DOMAttrModified event handlers, which allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have

3658	unspecified other impact via vectors involving removal of SVG elements.
CVE-2005-3182	Buffer overflow in the HTTP management interface for GFI MailSecurity 8.1 allows remote attackers to execute arbitrary code via long headers such as (1) Host and (2) Accept in HTTP requests. NOTE: the vendor suggests that this issues is "in an underlying Microsoft technology" which, if true, could mean that the overflow affects other products as well.
CVE-2013-1735	Use-after-free vulnerability in the mozilla::layout::ScrollbarActivity function in Mozilla Firefox before 24.0, Firefox ESR 17.x before 17.0.9, Thunderbird before 24.0, Thunderbird ESR 17.x before 17.0.9, and SeaMonkey before 2.21 allows remote attackers to execute arbitrary code via vectors related to image-document scrolling.
CVE-2012-0452	Use-after-free vulnerability in Mozilla Firefox 10.x before 10.0.1, Thunderbird 10.x before 10.0.1, and SeaMonkey 2.7 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via vectors that trigger failure of an nsXBLDocumentInfo::ReadPrototypeBindings function call, related to the cycle collector's access to a hash table containing a stale XBL binding.
CVE-2016-1521	The directrun function in directmachine.cpp in Libgraphite in Graphite 2 1.2.4, as used in Mozilla Firefox before 43.0 and Firefox ESR 38.x before 38.6.1, does not validate a certain skip operation, which allows remote attackers to execute arbitrary code, obtain sensitive information, or cause a denial of service (out-of-bounds read and application crash) via a crafted Graphite smart font.
CVE-2013-1730	Mozilla Firefox before 24.0, Firefox ESR 17.x before 17.0.9, Thunderbird before 24.0, Thunderbird ESR 17.x before 17.0.9, and SeaMonkey before 2.21 do not properly handle movement of XBL-backed nodes between documents, which allows remote attackers to execute arbitrary code or cause a denial of service (JavaScript compartment mismatch, or assertion failure and application exit) via a crafted web site.
CVE-2014-1538	Use-after-free vulnerability in the nsTextEditRules::CreateMozBR function in Mozilla Firefox before 30.0, Firefox ESR 24.x before 24.6, and Thunderbird before 24.6 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2013-1685	Use-after-free vulnerability in the nsIDocument::GetRootElement function in Mozilla Firefox before 22.0, Firefox ESR 17.x before 17.0.7, Thunderbird before 17.0.7, and Thunderbird ESR 17.x before 17.0.7 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via a crafted web site.
CVE-2013-5603	Use-after-free vulnerability in the nsContentUtils::ContentIsHostIncludingDescendantOf function in Mozilla Firefox before 25.0, Firefox ESR 24.x before 24.1, Thunderbird before 24.1, and SeaMonkey before 2.22 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via vectors involving HTML document templates.
CVE-2010-3181	Untrusted search path vulnerability in Mozilla Firefox before 3.5.14 and 3.6.x before 3.6.11, Thunderbird before 3.0.9 and 3.1.x before 3.1.5, and SeaMonkey before 2.0.9 on Windows allows local users to gain privileges via a Trojan horse DLL in the current working directory.
CVE-2012-3978	The nsLocation::CheckURL function in Mozilla Firefox before 15.0, Firefox ESR 10.x before 10.0.7, Thunderbird before 15.0, Thunderbird ESR 10.x before 10.0.7, and SeaMonkey before 2.12 does not properly follow the security model of the location object, which allows remote attackers to bypass intended content-loading restrictions or possibly have unspecified other impact via vectors involving chrome code.
CVE-2009-4630	Mozilla Necko, as used in Firefox, SeaMonkey, and other applications, performs DNS prefetching of domain names contained in links within local HTML documents, which makes it easier for remote attackers to determine the network location of the application's user by logging DNS requests. NOTE: the vendor disputes the significance of this issue, stating "I don't think we necessarily need to worry about that case."
CVE-2014-1510	The Web IDL implementation in Mozilla Firefox before 28.0, Firefox ESR 24.x before 24.4, Thunderbird before 24.4, and SeaMonkey before 2.25 allows remote attackers to execute arbitrary JavaScript code with chrome privileges by using an IDL fragment to trigger a window.open call.
CVE-2012-4187	Mozilla Firefox before 16.0, Firefox ESR 10.x before 10.0.8, Thunderbird before 16.0, Thunderbird ESR 10.x before 10.0.8, and SeaMonkey before 2.13 do not properly manage a certain insPos variable, which allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption and assertion failure) via unspecified vectors.
CVE-2006-2107	Buffer overflow in BL4 SMTP Server 0.1.4 and earlier allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a long argument to the (1) EHLO, (2) MAIL FROM, and (3) RCPT TO commands.
CVE-2011-2988	Buffer overflow in an unspecified string class in the WebGL shader implementation in Mozilla Firefox 4.x through 5, Thunderbird before 6, SeaMonkey 2.x before 2.3, and possibly other products allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a long source-code block for a shader.
CVE-2015-2721	Mozilla Network Security Services (NSS) before 3.19, as used in Mozilla Firefox before 39.0, Firefox ESR 31.x before 31.8 and 38.x before 38.1, Thunderbird before 38.1, and other products, does not properly determine state transitions for the TLS state machine, which allows man-in-the-middle attackers to defeat cryptographic protection mechanisms by blocking messages, as demonstrated by removing a forward-secrecy property by blocking a ServerKeyExchange message, aka a "SMACK SKIP-TLS" issue.
CVE-2012-3984	Mozilla Firefox before 16.0, Thunderbird before 16.0, and SeaMonkey before 2.13 do not properly handle navigation away from a web page that has a SELECT element's menu active, which allows remote attackers to spoof page content via vectors involving absolute positioning and scrolling.
CVE-2002-2436	The Cascading Style Sheets (CSS) implementation in Mozilla Firefox before 4.0, Thunderbird before 3.3, and SeaMonkey before 2.1 does not properly handle the :visited pseudo-class, which allows remote attackers to obtain sensitive information about visited web pages via a crafted HTML document, a related issue to CVE-2010-2264.
CVE-2013-1686	Use-after-free vulnerability in the mozilla::ResetDir function in Mozilla Firefox before 22.0, Firefox ESR 17.x before 17.0.7, Thunderbird before 17.0.7, and Thunderbird ESR 17.x before 17.0.7 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2014-	Buffer overflow in the _cairo_truetype_index_to_ucs4 function in cairo, as used in Mozilla Firefox before 28.0, Firefox ESR 24.x before 24.4, Thunderbird before 24.4, and SeaMonkey before 2.25, allows remote attackers to execute arbitrary code via a crafted extension

1509	that renders fonts in a PDF document.
CVE-2012-1954	Use-after-free vulnerability in the nsDocument::AdoptNode function in Mozilla Firefox 4.x through 13.0, Firefox ESR 10.x before 10.0.6, Thunderbird 5.0 through 13.0, Thunderbird ESR 10.x before 10.0.6, and SeaMonkey before 2.11 allows remote attackers to cause a denial of service (heap memory corruption) or possibly execute arbitrary code via vectors involving multiple adoptions and empty documents.
CVE-2005-0249	Heap-based buffer overflow in the DEC2EXE module for Symantec AntiVirus Library allows remote attackers to execute arbitrary code via a UPX compressed file containing a negative virtual offset to a crafted PE header.
CVE-2016-1526	The TtfUtil:LocaLookup function in TtfUtil.cpp in Libgraphite in Graphite 2 1.2.4, as used in Mozilla Firefox before 43.0 and Firefox ESR 38.x before 38.6.1, incorrectly validates a size value, which allows remote attackers to obtain sensitive information or cause a denial of service (out-of-bounds read and application crash) via a crafted Graphite smart font.
CVE-2016-1522	Code.cpp in Libgraphite in Graphite 2 1.2.4, as used in Mozilla Firefox before 43.0 and Firefox ESR 38.x before 38.6.1, does not consider recursive load calls during a size check, which allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly execute arbitrary code via a crafted Graphite smart font.
CVE-2013-5616	Use-after-free vulnerability in the nsEventListenerManager::HandleEventSubType function in Mozilla Firefox before 26.0, Firefox ESR 24.x before 24.2, Thunderbird before 24.2, and SeaMonkey before 2.23 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via vectors related to mListeners event listeners.
CVE-2013-0762	Use-after-free vulnerability in the imgRequest::OnStopFrame function in Mozilla Firefox before 18.0, Firefox ESR 10.x before 10.0.12 and 17.x before 17.0.1, Thunderbird before 17.0.2, Thunderbird ESR 10.x before 10.0.12 and 17.x before 17.0.1, and SeaMonkey before 2.15 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2014-8634	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 35.0, Firefox ESR 31.x before 31.4, Thunderbird before 31.4, and SeaMonkey before 2.32 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2005-0149	Thunderbird 0.6 through 0.9 and Mozilla 1.7 through 1.7.3 does not obey the network.cookie.disableCookieForMailNews preference, which could allow remote attackers bypass the user's intended privacy and security policy by using cookies in e-mail messages.
CVE-2013-0793	Mozilla Firefox before 20.0, Firefox ESR 17.x before 17.0.5, Thunderbird before 17.0.5, Thunderbird ESR 17.x before 17.0.5, and SeaMonkey before 2.17 do not ensure the correctness of the address bar during history navigation, which allows remote attackers to conduct cross-site scripting (XSS) attacks or phishing attacks by leveraging control over navigation timing.
CVE-2012-0458	Mozilla Firefox before 3.6.28 and 4.x through 10.0, Firefox ESR 10.x before 10.0.3, Thunderbird before 3.1.20 and 5.0 through 10.0, Thunderbird ESR 10.x before 10.0.3, and SeaMonkey before 2.8 do not properly restrict setting the home page through the dragging of a URL to the home button, which allows user-assisted remote attackers to execute arbitrary JavaScript code with chrome privileges via a javascript: URL that is later interpreted in the about:sessionrestore context.
CVE-2013-1687	The System Only Wrapper (SOW) and Chrome Object Wrapper (COW) implementations in Mozilla Firefox before 22.0, Firefox ESR 17.x before 17.0.7, Thunderbird before 17.0.7, and Thunderbird ESR 17.x before 17.0.7 do not properly restrict XBL user-defined functions, which allows remote attackers to execute arbitrary JavaScript code with chrome privileges, or conduct cross-site scripting (XSS) attacks, via a crafted web site.
CVE-2013-5618	Use-after-free vulnerability in the nsNodeUtils::LastRelease function in the table-editing user interface in the editor component in Mozilla Firefox before 26.0, Firefox ESR 24.x before 24.2, Thunderbird before 24.2, and SeaMonkey before 2.23 allows remote attackers to execute arbitrary code by triggering improper garbage collection.
CVE-2012-3105	The glBufferData function in the WebGL implementation in Mozilla Firefox 4.x through 12.0, Firefox ESR 10.x before 10.0.5, Thunderbird 5.0 through 12.0, Thunderbird ESR 10.x before 10.0.5, and SeaMonkey before 2.10 does not properly mitigate an unspecified flaw in an NVIDIA driver, which allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors, a related issue to CVE-2011-3101.
CVE-2000-0833	Buffer overflow in WinSMTP 1.06f and 2.X allows remote attackers to cause a denial of service via a long (1) USER or (2) HELO command.
CVE-2013-5604	The txXPathNodeUtils::getBaseURI function in the XSLT processor in Mozilla Firefox before 25.0, Firefox ESR 17.x before 17.0.10 and 24.x before 24.1, Thunderbird before 24.1, Thunderbird ESR 17.x before 17.0.10, and SeaMonkey before 2.22 does not properly initialize data, which allows remote attackers to execute arbitrary code or cause a denial of service (stack-based buffer overflow and application crash) via crafted documents.
CVE-2010-3182	A certain application-launch script in Mozilla Firefox before 3.5.14 and 3.6.x before 3.6.11, Thunderbird before 3.0.9 and 3.1.x before 3.1.5, and SeaMonkey before 2.0.9 on Linux places a zero-length directory name in the LD_LIBRARY_PATH, which allows local users to gain privileges via a Trojan horse shared library in the current working directory.
CVE-2013-1732	Buffer overflow in the nsFloatManager::GetFlowArea function in Mozilla Firefox before 24.0, Firefox ESR 17.x before 17.0.9, Thunderbird before 24.0, Thunderbird ESR 17.x before 17.0.9, and SeaMonkey before 2.21 allows remote attackers to execute arbitrary code via crafted use of lists and floats within a multi-column layout.
CVE-2012-1955	Mozilla Firefox 4.x through 13.0, Firefox ESR 10.x before 10.0.6, Thunderbird 5.0 through 13.0, Thunderbird ESR 10.x before 10.0.6, and SeaMonkey before 2.11 allow remote attackers to spoof the address bar via vectors involving history.forward and history.back calls.
CVE-2011-2989	The browser engine in Mozilla Firefox 4.x through 5, SeaMonkey 2.x before 2.3, Thunderbird before 6, and possibly other products does not properly implement WebGL, which allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unspecified vectors.
CVE-	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 7.0 and Thunderbird 7.0 allow remote attackers to cause a

2011-3651	denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2009-4629	Mozilla Necko, as used in Thunderbird 3.0.1, SeaMonkey, and other applications, performs DNS prefetching even when the app type is APP_TYPE_MAIL or APP_TYPE_EDITOR, which makes it easier for remote attackers to determine the network location of the application's user by logging DNS requests, as demonstrated by DNS requests triggered by reading text/plain e-mail messages in Thunderbird.
CVE-2012-3976	Mozilla Firefox before 15.0, Firefox ESR 10.x before 10.0.7, and SeaMonkey before 2.12 do not properly handle onLocationChange events during navigation between different https sites, which allows remote attackers to spoof the X.509 certificate information in the address bar via a crafted web page.
CVE-2013-0763	Use-after-free vulnerability in Mozilla Firefox before 18.0, Firefox ESR 17.x before 17.0.1, Thunderbird before 17.0.2, Thunderbird ESR 17.x before 17.0.1, and SeaMonkey before 2.15 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via vectors related to Mesa drivers and a resized WebGL canvas.
CVE-2014-1508	The libxul.so!gfxContext::Polygon function in Mozilla Firefox before 28.0, Firefox ESR 24.x before 24.4, Thunderbird before 24.4, and SeaMonkey before 2.25 allows remote attackers to obtain sensitive information from process memory, cause a denial of service (out-of-bounds read and application crash), or possibly bypass the Same Origin Policy via vectors involving MathML polygon rendering.
CVE-2012-4194	Mozilla Firefox before 16.0.2, Firefox ESR 10.x before 10.0.10, Thunderbird before 16.0.2, Thunderbird ESR 10.x before 10.0.10, and SeaMonkey before 2.13.2 do not prevent use of the valueOf method to shadow the location object (aka window.location), which makes it easier for remote attackers to conduct cross-site scripting (XSS) attacks via vectors involving a plugin.
CVE-2012-4205	Mozilla Firefox before 17.0, Thunderbird before 17.0, and SeaMonkey before 2.14 assign the system principal, rather than the sandbox principal, to XMLHttpRequest objects created in sandboxes, which allows remote attackers to conduct cross-site request forgery (CSRF) attacks or obtain sensitive information by leveraging a sandboxed add-on.
CVE-2006-0297	Multiple integer overflows in Mozilla Firefox 1.5, Thunderbird 1.5 if Javascript is enabled in mail, and SeaMonkey before 1.0 might allow remote attackers to execute arbitrary code via the (1) EscapeAttributeValue in jsxml.c for E4X, (2) nsSVGCairoSurface::Init in SVG, and (3) nsCanvasRenderingContext2D.cpp in Canvas.
CVE-2006-4567	Mozilla Firefox before 1.5.0.7 and Thunderbird before 1.5.0.7 makes it easy for users to accept self-signed certificates for the auto-update mechanism, which might allow remote user-assisted attackers to use DNS spoofing to trick users into visiting a malicious site and accepting a malicious certificate for the Mozilla update site, which can then be used to install arbitrary code on the next update.
CVE-2012-1956	Mozilla Firefox before 15.0, Thunderbird before 15.0, and SeaMonkey before 2.12 do not prevent use of the Object.defineProperty method to shadow the location object (aka window.location), which makes it easier for remote attackers to conduct cross-site scripting (XSS) attacks via vectors involving a plugin.
CVE-2002-1532	The administrative web interface (STEMWADM) for SurfControl SuperScout Email Filter allows remote attackers to cause a denial of service (resource exhaustion) via a GET request without the terminating /r/n/r/n (CRLF) sequence, which causes the interface to wait for the sequence and blocks other users from accessing it.
CVE-2014-1531	Use-after-free vulnerability in the nsGenericHTMLElement::GetWidthHeightForImage function in Mozilla Firefox before 29.0, Firefox ESR 24.x before 24.5, Thunderbird before 24.5, and SeaMonkey before 2.26 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via vectors involving an imgLoader object that is not properly handled during an image-resize operation.
CVE-2013-0771	Heap-based buffer overflow in the gfxTextRun::ShrinkToLigatureBoundaries function in Mozilla Firefox before 18.0, Firefox ESR 17.x before 17.0.1, Thunderbird before 17.0.2, Thunderbird ESR 17.x before 17.0.1, and SeaMonkey before 2.15 allows remote attackers to execute arbitrary code via a crafted document.
CVE-2013-1728	The IonMonkey JavaScript engine in Mozilla Firefox before 24.0, Thunderbird before 24.0, and SeaMonkey before 2.21, when Valgrind mode is used, does not properly initialize memory, which makes it easier for remote attackers to obtain sensitive information via unspecified vectors.
CVE-2011-0075	Unspecified vulnerability in the browser engine in Mozilla Firefox 3.5.x before 3.5.19 and 3.6.x before 3.6.17, Thunderbird before 3.1.10, and SeaMonkey before 2.0.14 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors, a different vulnerability than CVE-2011-0072, CVE-2011-0074, CVE-2011-0077, and CVE-2011-0078.
CVE-2010-1585	The nsIScriptableUnescapeHTML.parseFragment method in the ParanoidFragmentSink protection mechanism in Mozilla Firefox before 3.5.17 and 3.6.x before 3.6.14, Thunderbird before 3.1.8, and SeaMonkey before 2.0.12 does not properly sanitize HTML in a chrome document, which makes it easier for remote attackers to execute arbitrary JavaScript with chrome privileges via a javascript: URI in input to an extension, as demonstrated by a javascript:alert sequence in (1) the HREF attribute of an A element or (2) the ACTION attribute of a FORM element.
CVE-2012-0457	Use-after-free vulnerability in the nsSMILTimeValueSpec::ConvertBetweenTimeContainer function in Mozilla Firefox before 3.6.28 and 4.x through 10.0, Firefox ESR 10.x before 10.0.3, Thunderbird before 3.1.20 and 5.0 through 10.0, Thunderbird ESR 10.x before 10.0.3, and SeaMonkey before 2.8 might allow remote attackers to execute arbitrary code via an SVG animation.
CVE-2007-4296	Unspecified vulnerability in assp.pl in Anti-Spam SMTP Proxy Server (ASSP) 1.3.3 has unknown impact and attack vectors.
CVE-2012-3992	Mozilla Firefox before 16.0, Firefox ESR 10.x before 10.0.8, Thunderbird before 16.0, Thunderbird ESR 10.x before 10.0.8, and SeaMonkey before 2.13 do not properly manage history data, which allows remote attackers to conduct cross-site scripting (XSS) attacks or obtain sensitive POST content via vectors involving a location.hash write operation and history navigation that triggers the loading of a URL into the history object.
CVE-2013-0746	Mozilla Firefox before 18.0, Firefox ESR 10.x before 10.0.12 and 17.x before 17.0.2, Thunderbird before 17.0.2, Thunderbird ESR 10.x before 10.0.12 and 17.x before 17.0.2, and SeaMonkey before 2.15 do not properly implement quickstubs that use the jsval data type for their return values, which allows remote attackers to execute arbitrary code or cause a denial of service (compartment mismatch and application crash) via crafted JavaScript code that is not properly handled during garbage collection.
CVE-	The Content Security Policy (CSP) functionality in Mozilla Firefox 4.x through 13.0, Firefox ESR 10.x before 10.0.6, Thunderbird 5.0

2012-1963	through 13.0, Thunderbird ESR 10.x before 10.0.6, and SeaMonkey before 2.11 does not properly restrict the strings placed into the blocked-uri parameter of a violation report, which allows remote web servers to capture OpenID credentials and OAuth 2.0 access tokens by triggering a violation.
CVE-2013-0801	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 21.0, Firefox ESR 17.x before 17.0.6, Thunderbird before 17.0.6, and Thunderbird ESR 17.x before 17.0.6 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2011-2363	Use-after-free vulnerability in the nsSVGPointList::AppendElement function in the implementation of SVG element lists in Mozilla Firefox before 3.6.18, Thunderbird before 3.1.11, and SeaMonkey through 2.0.14 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via vectors involving a user-supplied callback.
CVE-2010-2765	Integer overflow in the FRAMESET element implementation in Mozilla Firefox before 3.5.12 and 3.6.x before 3.6.9, Thunderbird before 3.0.7 and 3.1.x before 3.1.3, and SeaMonkey before 2.0.7 might allow remote attackers to execute arbitrary code via a large number of values in the cols (aka columns) attribute, leading to a heap-based buffer overflow.
CVE-2005-1931	GoodTech SMTP Server 5.14 allows remote attackers to cause a denial of service (application crash) via a RCPT TO command with an invalid argument, as demonstrated using an "A" character.
CVE-2010-0179	Mozilla Firefox before 3.0.19 and 3.5.x before 3.5.8, and SeaMonkey before 2.0.3, when the XMLHttpRequestSpy module in the Firebug add-on is used, does not properly handle interaction between the XMLHttpRequestSpy object and chrome privileged objects, which allows remote attackers to execute arbitrary JavaScript via a crafted HTTP response.
CVE-2009-1840	Mozilla Firefox before 3.0.11, Thunderbird, and SeaMonkey do not check content policy before loading a script file into a XUL document, which allows remote attackers to bypass intended access restrictions via a crafted HTML document, as demonstrated by a "web bug" in an e-mail message, or web script or an advertisement in a web page.
CVE-2016-1523	The SillMap::readFace function in FeatureMap.cpp in Libgraphite in Graphite 2 1.2.4, as used in Mozilla Firefox before 43.0 and Firefox ESR 38.x before 38.6.1, mishandles a return value, which allows remote attackers to cause a denial of service (missing initialization, NULL pointer dereference, and application crash) via a crafted Graphite smart font.
CVE-2008-2831	Multiple cross-site scripting (XSS) vulnerabilities in the delegated spam management feature in the Spam Quarantine Management (SQM) component in MailMarshal SMTP 6.0.3.8 through 6.3.0.0 allow user-assisted remote authenticated users to inject arbitrary web script or HTML via (1) the list of blocked senders or (2) the list of safe senders.
CVE-2007-0008	Integer underflow in the SSLv2 support in Mozilla Network Security Services (NSS) before 3.11.5, as used by Firefox before 1.5.0.10 and 2.x before 2.0.0.2, SeaMonkey before 1.0.8, Thunderbird before 1.5.0.10, and certain Sun Java System server products before 20070611, allows remote attackers to execute arbitrary code via a crafted SSLv2 server message containing a public key that is too short to encrypt the "Master Secret", which results in a heap-based overflow.
CVE-2012-3966	Mozilla Firefox before 15.0, Firefox ESR 10.x before 10.0.7, Thunderbird before 15.0, Thunderbird ESR 10.x before 10.0.7, and SeaMonkey before 2.12 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a negative height value in a BMP image within a .ICO file, related to (1) improper handling of the transparency bitmask by the nsICODecoder component and (2) improper processing of the alpha channel by the nsBMPDecoder component.
CVE-2014-1532	Use-after-free vulnerability in the nsHostResolver::ConditionallyRefreshRecord function in libxul.so in Mozilla Firefox before 29.0, Firefox ESR 24.x before 24.5, Thunderbird before 24.5, and SeaMonkey before 2.26 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via vectors related to host resolution.
CVE-2011-0074	Unspecified vulnerability in the browser engine in Mozilla Firefox 3.5.x before 3.5.19 and 3.6.x before 3.6.17, Thunderbird before 3.1.10, and SeaMonkey before 2.0.14 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors, a different vulnerability than CVE-2011-0072, CVE-2011-0075, CVE-2011-0077, and CVE-2011-0078.
CVE-2009-1841	js/src/xpconnect/src/xpcwrappedjsclass.cpp in Mozilla Firefox before 3.0.11, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.17 allows remote attackers to execute arbitrary web script with the privileges of a chrome object, as demonstrated by the browser sidebar and the FeedWriter.
CVE-2013-5609	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 26.0, Firefox ESR 24.x before 24.2, Thunderbird before 24.2, and SeaMonkey before 2.23 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2015-2739	The ArrayBufferBuilder::append function in Mozilla Firefox before 39.0, Firefox ESR 31.x before 31.8 and 38.x before 38.1, and Thunderbird before 38.1 accesses unintended memory locations, which has unspecified impact and attack vectors.
CVE-2012-3991	Mozilla Firefox before 16.0, Firefox ESR 10.x before 10.0.8, Thunderbird before 16.0, Thunderbird ESR 10.x before 10.0.8, and SeaMonkey before 2.13 do not properly restrict JSAPI access to the GetProperty function, which allows remote attackers to bypass the Same Origin Policy and possibly have unspecified other impact via a crafted web site.
CVE-2015-0797	GStreamer before 1.4.5, as used in Mozilla Firefox before 38.0, Firefox ESR 31.x before 31.7, and Thunderbird before 31.7 on Linux, allows remote attackers to cause a denial of service (buffer over-read and application crash) or possibly execute arbitrary code via crafted H.264 video data in an m4v file.
CVE-2007-1282	Integer overflow in Mozilla Thunderbird before 1.5.0.10 and SeaMonkey before 1.0.8 allows remote attackers to trigger a buffer overflow and possibly execute arbitrary code via a text/enhanced or text/richtext e-mail message with an extremely long line.
CVE-2008-2785	Mozilla Firefox before 2.0.0.16 and 3.x before 3.0.1, Thunderbird before 2.0.0.16, and SeaMonkey before 1.1.11 use an incorrect integer data type as a CSS object reference counter in the CSSValue array (aka nsCSSValue:Array) data structure, which allows remote attackers to execute arbitrary code via a large number of references to a common CSS object, leading to a counter overflow and a free of in-use memory, aka ZDI-CAN-349.
CVE-	The certificate-warning functionality in browser/components/certerror/content/aboutCertError.xhtml in Mozilla Firefox 4.x through 12.0,

2012-1964	Firefox ESR 10.x before 10.0.6, Thunderbird 5.0 through 12.0, Thunderbird ESR 10.x before 10.0.6, and SeaMonkey before 2.10 does not properly handle attempted clickjacking of the about:certerror page, which allows man-in-the-middle attackers to trick users into adding an unintended exception via an IFRAME element.
CVE-2014-1487	The Web workers implementation in Mozilla Firefox before 27.0, Firefox ESR 24.x before 24.3, Thunderbird before 24.3, and SeaMonkey before 2.24 allows remote attackers to bypass the Same Origin Policy and obtain sensitive authentication information via vectors involving error messages.
CVE-2012-0456	The SVG Filters implementation in Mozilla Firefox before 3.6.28 and 4.x through 10.0, Firefox ESR 10.x before 10.0.3, Thunderbird before 3.1.20 and 5.0 through 10.0, Thunderbird ESR 10.x before 10.0.3, and SeaMonkey before 2.8 might allow remote attackers to obtain sensitive information from process memory via vectors that trigger an out-of-bounds read.
CVE-2009-1836	Mozilla Firefox before 3.0.11, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.17 use the HTTP Host header to determine the context of a document provided in a non-200 CONNECT response from a proxy server, which allows man-in-the-middle attackers to execute arbitrary web script by modifying this CONNECT response, aka an "SSL tampering" attack.
CVE-2013-1725	Mozilla Firefox before 24.0, Firefox ESR 17.x before 17.0.9, Thunderbird before 24.0, Thunderbird ESR 17.x before 17.0.9, and SeaMonkey before 2.21 do not ensure that initialization occurs for JavaScript objects with compartments, which allows remote attackers to execute arbitrary code by leveraging incorrect scope handling.
CVE-2015-0815	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 37.0, Firefox ESR 31.x before 31.6, and Thunderbird before 31.6 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2010-2764	Mozilla Firefox before 3.5.12 and 3.6.x before 3.6.9, Thunderbird before 3.0.7 and 3.1.x before 3.1.3, and SeaMonkey before 2.0.7 do not properly restrict read access to the statusText property of XMLHttpRequest objects, which allows remote attackers to discover the existence of intranet web servers via cross-origin requests.
CVE-2016-1952	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2013-0747	The gPluginHandler.handleEvent function in the plugin handler in Mozilla Firefox before 18.0, Firefox ESR 17.x before 17.0.2, Thunderbird before 17.0.2, Thunderbird ESR 17.x before 17.0.2, and SeaMonkey before 2.15 does not properly enforce the Same Origin Policy, which allows remote attackers to conduct clickjacking attacks via crafted JavaScript code that listens for a mutation event.
CVE-1999-1516	A buffer overflow in TenFour TFS Gateway SMTP mail server 3.2 allows an attacker to crash the mail server and possibly execute arbitrary code by offering more than 128 bytes in a MAIL FROM string.
CVE-2011-0085	Use-after-free vulnerability in the nsXULCommandDispatcher function in Mozilla Firefox before 3.6.18, Thunderbird before 3.1.11, and SeaMonkey through 2.0.14 allows remote attackers to execute arbitrary code via a crafted XUL document that dequeues the current command updater.
CVE-2012-1970	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 15.0, Firefox ESR 10.x before 10.0.7, Thunderbird before 15.0, Thunderbird ESR 10.x before 10.0.7, and SeaMonkey before 2.12 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2006-3216	Clearswift MAILsweeper for SMTP before 4.3.20 and MAILsweeper for Exchange before 4.3.20 allows remote attackers to cause a denial of service via (1) non-ASCII characters in a reverse DNS lookup result from a Received header, which leads to a Receiver service stop, and (2) unspecified vectors involving malformed messages, which causes "unpredictable behavior" that prevents the Security service from processing more messages.
CVE-2012-0445	Mozilla Firefox 4.x through 9.0, Thunderbird 5.0 through 9.0, and SeaMonkey before 2.7 allow remote attackers to bypass the HTML5 frame-navigation policy and replace arbitrary sub-frames by creating a form submission target with a sub-frame's name attribute.
CVE-2005-0107	bsmtpd 2.3 and earlier does not properly sanitize e-mail addresses, which allows remote attackers to execute arbitrary commands.
CVE-2013-1726	Mozilla Updater in Mozilla Firefox before 24.0, Firefox ESR 17.x before 17.0.9, Thunderbird before 24.0, Thunderbird ESR 17.x before 17.0.9, and SeaMonkey before 2.21 does not ensure exclusive access to a MAR file, which allows local users to gain privileges by creating a Trojan horse file after MAR signature verification but before MAR use.
CVE-2015-2734	The CairoTextureClientD3D9::BorrowDrawTarget function in the Direct3D 9 implementation in Mozilla Firefox before 39.0, Firefox ESR 31.x before 31.8 and 38.x before 38.1, and Thunderbird before 38.1 reads data from uninitialized memory locations, which has unspecified impact and attack vectors.
CVE-2009-2462	The browser engine in Mozilla Firefox before 3.0.12 and Thunderbird allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to (1) the frame chain and synchronous events, (2) a SetMayHaveFrame assertion and nsCSSFrameConstructor::CreateFloatingLetterFrame, (3) nsCSSFrameConstructor::ConstructFrame, (4) the child list and initial reflow, (5) GetLastSpecialSibling, (6) nsFrameManager::GetPrimaryFrameFor and MathML, (7) nsFrame::GetBoxAscent, (8) nsCSSFrameConstructor::AdjustParentFrame, (9) nsDOMOfflineResourceList, and (10) nsContentUtils::ComparePosition.
CVE-2014-1486	Use-after-free vulnerability in the imgRequestProxy function in Mozilla Firefox before 27.0, Firefox ESR 24.x before 24.3, Thunderbird before 24.3, and SeaMonkey before 2.24 allows remote attackers to execute arbitrary code via vectors involving unspecified Content-Type values for image data.
CVE-2008-0591	Mozilla Firefox before 2.0.0.12 and Thunderbird before 2.0.0.12 does not properly manage a delay timer used in confirmation dialogs, which might allow remote attackers to trick users into confirming an unsafe action, such as remote file execution, by using a timer to change the window focus, aka the "dialog refocus bug" or "ffclick2".

CVE-2011-2378	The appendChild function in Mozilla Firefox before 3.6.20, Thunderbird 3.x before 3.1.12, SeaMonkey 2.x, and possibly other products does not properly handle DOM objects, which allows remote attackers to execute arbitrary code via unspecified vectors that lead to dereferencing of a "dangling pointer."
CVE-2012-3967	The WebGL implementation in Mozilla Firefox before 15.0, Firefox ESR 10.x before 10.0.7, Thunderbird before 15.0, Thunderbird ESR 10.x before 10.0.7, and SeaMonkey before 2.12 on Linux, when a large number of sampler uniforms are used, does not properly interact with Mesa drivers, which allows remote attackers to execute arbitrary code or cause a denial of service (stack memory corruption) via a crafted web site.
CVE-2012-0444	Mozilla Firefox before 3.6.26 and 4.x through 9.0, Thunderbird before 3.1.18 and 5.0 through 9.0, and SeaMonkey before 2.7 do not properly initialize nsChildView data structures, which allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via a crafted Ogg Vorbis file.
CVE-2007-6573	QK SMTP Server 3 allows remote attackers to cause a denial of service (daemon crash) via a long (1) HELO, (2) MAIL FROM, or (3) RCPT TO command; or (4) a long string in the message sent after the DATA command; possibly a related issue to CVE-2006-5551.
CVE-2000-0738	WebShield SMTP 4.5 allows remote attackers to cause a denial of service by sending e-mail with a From: address that has a . (period) at the end, which causes WebShield to continuously send itself copies of the e-mail.
CVE-2012-0467	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 4.x through 11.0, Firefox ESR 10.x before 10.0.4, Thunderbird 5.0 through 11.0, Thunderbird ESR 10.x before 10.0.4, and SeaMonkey before 2.9 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2010-0182	The XMLDocument::load function in Mozilla Firefox before 3.5.9 and 3.6.x before 3.6.2, Thunderbird before 3.0.4, and SeaMonkey before 2.0.4 does not perform the expected nsIContentPolicy checks during loading of content by XML documents, which allows attackers to bypass intended access restrictions via crafted content.
CVE-2011-2362	Mozilla Firefox before 3.6.18, Thunderbird before 3.1.11, and SeaMonkey through 2.0.14 do not distinguish between cookies for two domain names that differ only in a trailing dot, which allows remote web servers to bypass the Same Origin Policy via Set-Cookie headers.
CVE-2009-1838	The garbage-collection implementation in Mozilla Firefox before 3.0.11, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.17 sets an element's owner document to null in unspecified circumstances, which allows remote attackers to execute arbitrary JavaScript with chrome privileges via a crafted event handler, related to an incorrect context for this event handler.
CVE-2012-3990	Use-after-free vulnerability in the IME State Manager implementation in Mozilla Firefox before 16.0, Firefox ESR 10.x before 10.0.8, Thunderbird before 16.0, Thunderbird ESR 10.x before 10.0.8, and SeaMonkey before 2.13 allows remote attackers to execute arbitrary code via unspecified vectors, related to the nsIContent::GetNameSpaceID function.
CVE-2013-0784	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 19.0, Thunderbird before 17.0.3, and SeaMonkey before 2.16 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2013-0748	The XBL.__proto__.toString implementation in Mozilla Firefox before 18.0, Firefox ESR 10.x before 10.0.12 and 17.x before 17.0.2, Thunderbird before 17.0.2, Thunderbird ESR 10.x before 10.0.12 and 17.x before 17.0.2, and SeaMonkey before 2.15 makes it easier for remote attackers to bypass the ASLR protection mechanism by calling the toString function of an XBL object.
CVE-2010-2763	The XPCSafeJSObjectWrapper class in the SafeJSObjectWrapper (aka SJOW) implementation in Mozilla Firefox before 3.5.12, Thunderbird before 3.0.7, and SeaMonkey before 2.0.7 does not properly restrict scripted functions, which allows remote attackers to bypass the Same Origin Policy and conduct cross-site scripting (XSS) attacks via a crafted function.
CVE-2011-0072	Unspecified vulnerability in the browser engine in Mozilla Firefox 3.5.x before 3.5.19 and 3.6.x before 3.6.17, Thunderbird before 3.1.10, and SeaMonkey before 2.0.14 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors, a different vulnerability than CVE-2011-0074, CVE-2011-0075, CVE-2011-0077, and CVE-2011-0078.
CVE-2012-0443	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 4.x through 9.0, Thunderbird 5.0 through 9.0, and SeaMonkey before 2.7 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2013-1722	Use-after-free vulnerability in the nsAnimationManager::BuildAnimations function in the Animation Manager in Mozilla Firefox before 24.0, Firefox ESR 17.x before 17.0.9, Thunderbird before 24.0, Thunderbird ESR 17.x before 17.0.9, and SeaMonkey before 2.21 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via vectors involving stylesheet cloning.
CVE-2002-2121	SurfControl SuperScout Email filter for SMTP 3.5.1 allows remote attackers to cause a denial of service (crash) via a long SMTP (1) HELO or (2) RCPT TO command, possibly due to a buffer overflow.
CVE-2013-1718	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 24.0, Firefox ESR 17.x before 17.0.9, Thunderbird before 24.0, Thunderbird ESR 17.x before 17.0.9, and SeaMonkey before 2.21 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2011-3232	YARR, as used in Mozilla Firefox before 7.0, Thunderbird before 7.0, and SeaMonkey before 2.4, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via crafted JavaScript.
CVE-2011-0053	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 3.5.17 and 3.6.x before 3.6.14, Thunderbird before 3.1.8, and SeaMonkey before 2.0.12 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2013-1670	The Chrome Object Wrapper (COW) implementation in Mozilla Firefox before 21.0, Firefox ESR 17.x before 17.0.6, Thunderbird before 17.0.6, and Thunderbird ESR 17.x before 17.0.6 does not prevent acquisition of chrome privileges during calls to content level constructors, which allows remote attackers to bypass certain read-only restrictions and conduct cross-site scripting (XSS) attacks via

	a crafted web site.
CVE-2012-3969	Integer overflow in the nsSVGFEMorphologyElement::Filter function in Mozilla Firefox before 15.0, Firefox ESR 10.x before 10.0.7, Thunderbird before 15.0, Thunderbird ESR 10.x before 10.0.7, and SeaMonkey before 2.12 allows remote attackers to execute arbitrary code via a crafted SVG filter that triggers an incorrect sum calculation, leading to a heap-based buffer overflow.
CVE-2014-1559	Mozilla Firefox before 31.0 and Thunderbird before 31.0 allow remote attackers to cause a denial of service (X.509 certificate parsing outage) via a crafted certificate that does not use UTF-8 character encoding in a required context, a different vulnerability than CVE-2014-1558.
CVE-2012-1960	The qcms_transform_data_rgb_out_lut_sse2 function in the QCMS implementation in Mozilla Firefox 4.x through 13.0, Thunderbird 5.0 through 13.0, and SeaMonkey before 2.11 might allow remote attackers to obtain sensitive information from process memory via a crafted color profile that triggers an out-of-bounds read operation.
CVE-2016-1964	Use-after-free vulnerability in the AtomicBaseIncDec function in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) by leveraging mishandling of XML transformations.
CVE-2013-1723	The NativeKey widget in Mozilla Firefox before 24.0, Thunderbird before 24.0, and SeaMonkey before 2.21 processes key messages after destruction by a dispatched event listener, which allows remote attackers to cause a denial of service (application crash) by leveraging incorrect event usage after widget-memory reallocation.
CVE-2007-4038	Argument injection vulnerability in Mozilla Firefox before 2.0.0.5, when running on systems with Thunderbird 1.5 installed and certain URIs registered, allows remote attackers to conduct cross-browser scripting attacks and execute arbitrary commands via shell metacharacters in a mailto URI, which are inserted into the command line that is created when invoking Thunderbird.exe, a similar issue to CVE-2007-3670.
CVE-2012-1971	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 15.0, Thunderbird before 15.0, and SeaMonkey before 2.12 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to garbage collection after certain MethodJIT execution, and unknown other vectors.
CVE-2015-0836	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 36.0, Firefox ESR 31.x before 31.5, and Thunderbird before 31.5 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2013-0768	Stack-based buffer overflow in the Canvas implementation in Mozilla Firefox before 18.0, Firefox ESR 17.x before 17.0.2, Thunderbird before 17.0.2, Thunderbird ESR 17.x before 17.0.2, and SeaMonkey before 2.15 allows remote attackers to execute arbitrary code via an HTML document that specifies invalid width and height values.
CVE-2015-0801	Mozilla Firefox before 37.0, Firefox ESR 31.x before 31.6, and Thunderbird before 31.6 allow remote attackers to bypass the Same Origin Policy and execute arbitrary JavaScript code with chrome privileges via vectors involving anchor navigation, a similar issue to CVE-2015-0818.
CVE-2010-2753	Integer overflow in Mozilla Firefox 3.5.x before 3.5.11 and 3.6.x before 3.6.7, Thunderbird 3.0.x before 3.0.6 and 3.1.x before 3.1.1, and SeaMonkey before 2.0.6 allows remote attackers to execute arbitrary code via a large selection attribute in a XUL tree element, which triggers a use-after-free.
CVE-2011-2980	Untrusted search path vulnerability in the ThinkPadSensor::Startup function in Mozilla Firefox before 3.6.20, Thunderbird 3.x before 3.1.12, allows local users to gain privileges by leveraging write access in an unspecified directory to place a Trojan horse DLL that is loaded into the running Firefox process.
CVE-2014-8638	The navigator.sendBeacon implementation in Mozilla Firefox before 35.0, Firefox ESR 31.x before 31.4, Thunderbird before 31.4, and SeaMonkey before 2.32 omits the CORS Origin header, which allows remote attackers to bypass intended CORS access-control checks and conduct cross-site request forgery (CSRF) attacks via a crafted web site.
CVE-2012-1961	Mozilla Firefox 4.x through 13.0, Firefox ESR 10.x before 10.0.6, Thunderbird 5.0 through 13.0, Thunderbird ESR 10.x before 10.0.6, and SeaMonkey before 2.11 do not properly handle duplicate values in X-Frame-Options headers, which makes it easier for remote attackers to conduct clickjacking attacks via a FRAME element referencing a web site that produces these duplicate values.
CVE-2010-1207	Mozilla Firefox before 3.6.7 and Thunderbird before 3.1.1 do not properly implement read restrictions for CANVAS elements, which allows remote attackers to obtain sensitive cross-origin information via vectors involving reference retention and node deletion.
CVE-2014-1558	Mozilla Firefox before 31.0 and Thunderbird before 31.0 allow remote attackers to cause a denial of service (X.509 certificate parsing outage) via a crafted certificate that does not use UTF-8 character encoding in a required context, a different vulnerability than CVE-2014-1559.
CVE-2005-4809	Mozilla Firefox 1.0.1 and possibly other versions, including Mozilla and Thunderbird, allows remote attackers to spoof the URL in the Status Bar via an A HREF tag that contains a TABLE tag that contains another A tag.
CVE-2010-3776	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 3.5.16 and 3.6.x before 3.6.13, Thunderbird before 3.0.11 and 3.1.x before 3.1.7, and SeaMonkey before 2.0.11 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2010-2762	The XPCSafeJSObjectWrapper class in the SafeJSObjectWrapper (aka SJOW) implementation in Mozilla Firefox 3.6.x before 3.6.9 and Thunderbird 3.1.x before 3.1.3 does not properly restrict objects at the end of scope chains, which allows remote attackers to execute arbitrary JavaScript code with chrome privileges via vectors related to a chrome privileged object and a chain ending in an outer object.
CVE-2013-1724	Use-after-free vulnerability in the mozilla::dom::HTMLFormElement::IsDefaultSubmitElement function in Mozilla Firefox before 24.0, Thunderbird before 24.0, and SeaMonkey before 2.21 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via vectors involving a destroyed SELECT element.
CVE-2015-	Mozilla Firefox before 37.0, Firefox ESR 31.x before 31.6, and Thunderbird before 31.6 do not properly restrict resource: URLs, which makes it easier for remote attackers to execute arbitrary JavaScript code with chrome privileges by leveraging the ability to bypass the

0816	Same Origin Policy, as demonstrated by the resource: URL associated with PDF.js.
CVE-2011-0071	Directory traversal vulnerability in Mozilla Firefox before 3.5.19 and 3.6.x before 3.6.17, Thunderbird before 3.1.10, and SeaMonkey before 2.0.14 on Windows allows remote attackers to determine the existence of arbitrary files, and possibly load resources, via vectors involving a resource: URL.
CVE-2013-0769	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 18.0, Firefox ESR 10.x before 10.0.12 and 17.x before 17.0.1, Thunderbird before 17.0.2, Thunderbird ESR 10.x before 10.0.12 and 17.x before 17.0.1, and SeaMonkey before 2.15 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2007-3735	Multiple unspecified vulnerabilities in the JavaScript engine in Mozilla Firefox before 2.0.0.5 and Thunderbird before 2.0.0.5 allow remote attackers to cause a denial of service (crash) via unspecified vectors that trigger memory corruption.
CVE-2012-4207	The HZ-GB-2312 character-set implementation in Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0, Thunderbird ESR 10.x before 10.0.11, and SeaMonkey before 2.14 does not properly handle a ~ (tilde) character in proximity to a chunk delimiter, which allows remote attackers to conduct cross-site scripting (XSS) attacks via a crafted document.
CVE-2016-1960	Integer underflow in the nsHtml5TreeBuilder class in the HTML5 string parser in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7 allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free) by leveraging mishandling of end tags, as demonstrated by incorrect SVG processing, aka ZDI-CAN-3545.
CVE-2013-0783	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 19.0, Firefox ESR 17.x before 17.0.3, Thunderbird before 17.0.3, Thunderbird ESR 17.x before 17.0.3, and SeaMonkey before 2.16 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2013-0744	Use-after-free vulnerability in the TableBackgroundPainter::TableBackgroundData::Destroy function in Mozilla Firefox before 18.0, Firefox ESR 10.x before 10.0.12 and 17.x before 17.0.2, Thunderbird before 17.0.2, Thunderbird ESR 10.x before 10.0.12 and 17.x before 17.0.2, and SeaMonkey before 2.15 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via an HTML document with a table containing many columns and column groups.
CVE-2012-0455	Mozilla Firefox before 3.6.28 and 4.x through 10.0, Firefox ESR 10.x before 10.0.3, Thunderbird before 3.1.20 and 5.0 through 10.0, Thunderbird ESR 10.x before 10.0.3, and SeaMonkey before 2.8 do not properly restrict drag-and-drop operations on javascript: URLs, which allows user-assisted remote attackers to conduct cross-site scripting (XSS) attacks via a crafted web page, related to a "DragAndDropJacking" issue.
CVE-2012-3989	Mozilla Firefox before 16.0, Thunderbird before 16.0, and SeaMonkey before 2.13 do not properly perform a cast of an unspecified variable during use of the instanceof operator on a JavaScript object, which allows remote attackers to execute arbitrary code or cause a denial of service (assertion failure) via a crafted web site.
CVE-2012-3968	Use-after-free vulnerability in the WebGL implementation in Mozilla Firefox before 15.0, Firefox ESR 10.x before 10.0.7, Thunderbird before 15.0, Thunderbird ESR 10.x before 10.0.7, and SeaMonkey before 2.12 allows remote attackers to execute arbitrary code via vectors related to deletion of a fragment shader by its accessor.
CVE-2010-2752	Integer overflow in an array class in Mozilla Firefox 3.5.x before 3.5.11 and 3.6.x before 3.6.7, Thunderbird 3.0.x before 3.0.6 and 3.1.x before 3.1.1, and SeaMonkey before 2.0.6 allows remote attackers to execute arbitrary code by placing many Cascading Style Sheets (CSS) values in an array, related to references to external font resources and an inconsistency between 16-bit and 32-bit integers.
CVE-2011-2981	The event-management implementation in Mozilla Firefox before 3.6.20, SeaMonkey 2.x, Thunderbird 3.x before 3.1.12, and possibly other products does not properly select the context for script to run in, which allows remote attackers to bypass the Same Origin Policy or execute arbitrary JavaScript code with chrome privileges via a crafted web site.
CVE-2011-2364	Unspecified vulnerability in the browser engine in Mozilla Firefox 3.6.x before 3.6.18 and Thunderbird before 3.1.11 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors, a different vulnerability than CVE-2011-2365.
CVE-2014-1482	RasterImage.cpp in Mozilla Firefox before 27.0, Firefox ESR 24.x before 24.3, Thunderbird before 24.3, and SeaMonkey before 2.24 does not prevent access to discarded data, which allows remote attackers to execute arbitrary code or cause a denial of service (incorrect write operations) via crafted image data, as demonstrated by Goo Create.
CVE-2014-1560	Mozilla Firefox before 31.0 and Thunderbird before 31.0 allow remote attackers to cause a denial of service (X.509 certificate parsing outage) via a crafted certificate that does not use ASCII character encoding in a required context.
CVE-2015-4000	The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite is enabled on a server but not on a client, does not properly convey a DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a ClientHello with DHE replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the "Logjam" issue.
CVE-2012-3988	Use-after-free vulnerability in Mozilla Firefox before 16.0, Firefox ESR 10.x before 10.0.8, Thunderbird before 16.0, Thunderbird ESR 10.x before 10.0.8, and SeaMonkey before 2.13 might allow user-assisted remote attackers to execute arbitrary code via vectors involving use of mozRequestFullScreen to enter full-screen mode, and use of the history.back method for backwards history navigation.
CVE-2012-3971	Summer Institute of Linguistics (SIL) Graphite 2, as used in Mozilla Firefox before 15.0, Thunderbird before 15.0, and SeaMonkey before 2.12, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via vectors related to the (1) Silf::readClassMap and (2) Pass::readPass functions.
CVE-2010-3777	Unspecified vulnerability in Mozilla Firefox 3.6.x before 3.6.13 and Thunderbird 3.1.x before 3.1.7 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2010-3178	Mozilla Firefox before 3.5.14 and 3.6.x before 3.6.11, Thunderbird before 3.0.9 and 3.1.x before 3.1.5, and SeaMonkey before 2.0.9 do not properly handle certain modal calls made by javascript: URLs in circumstances related to opening a new window and performing cross-domain navigation, which allows remote attackers to bypass the Same Origin Policy via a crafted HTML document.
CVE-	Heap-based buffer overflow in the mozilla::gfx::CopyRect function in Mozilla Firefox before 36.0, Firefox ESR 31.x before 31.5, and

2015-0827	Thunderbird before 31.5 allows remote attackers to obtain sensitive information from uninitialized process memory via a malformed SVG graphic.
CVE-2012-1962	Use-after-free vulnerability in the JSDependentString::undepend function in Mozilla Firefox 4.x through 13.0, Firefox ESR 10.x before 10.0.6, Thunderbird 5.0 through 13.0, Thunderbird ESR 10.x before 10.0.6, and SeaMonkey before 2.11 allows remote attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via vectors involving strings with multiple dependencies.
CVE-2011-0070	Unspecified vulnerability in the browser engine in Mozilla Firefox 3.5.x before 3.5.19, 3.6.x before 3.6.17, and 4.x before 4.0.1; Thunderbird before 3.1.10; and SeaMonkey before 2.0.14 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors, a different vulnerability than CVE-2011-0069.
CVE-2014-1481	Mozilla Firefox before 27.0, Firefox ESR 24.x before 24.3, Thunderbird before 24.3, and SeaMonkey before 2.24 allow remote attackers to bypass intended restrictions on window objects by leveraging inconsistency in native getter methods across different JavaScript engines.
CVE-2016-1953	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 45.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to js/src/jit/arm/Assembler-arm.cpp, and unknown other vectors.
CVE-2012-0442	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 3.6.26 and 4.x through 9.0, Thunderbird before 3.1.18 and 5.0 through 9.0, and SeaMonkey before 2.7 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2013-1720	The nsHtml5TreeBuilder::resetTheInsertionMode function in the HTML5 Tree Builder in Mozilla Firefox before 24.0, Thunderbird before 24.0, and SeaMonkey before 2.21 does not properly maintain the state of the insertion-mode stack for template elements, which allows remote attackers to execute arbitrary code or cause a denial of service (heap-based buffer over-read) by triggering use of this stack in its empty state.
CVE-2013-0781	Use-after-free vulnerability in the nsPrintEngine::CommonPrint function in Mozilla Firefox before 19.0, Thunderbird before 17.0.3, and SeaMonkey before 2.16 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2013-1672	The Mozilla Maintenance Service in Mozilla Firefox before 21.0, Firefox ESR 17.x before 17.0.6, Thunderbird before 17.0.6, and Thunderbird ESR 17.x before 17.0.6 on Windows allows local users to bypass integrity verification and gain privileges via vectors involving junctions.
CVE-2012-1972	Use-after-free vulnerability in the nsHTMLEditor::CollapseAdjacentTextNodes function in Mozilla Firefox before 15.0, Firefox ESR 10.x before 10.0.7, Thunderbird before 15.0, Thunderbird ESR 10.x before 10.0.7, and SeaMonkey before 2.12 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2010-2760	Use-after-free vulnerability in the nsTreeSelection function in Mozilla Firefox before 3.5.12 and 3.6.x before 3.6.9, Thunderbird before 3.0.7 and 3.1.x before 3.1.3, and SeaMonkey before 2.0.7 might allow remote attackers to execute arbitrary code via vectors involving a XUL tree selection, related to a "dangling pointer vulnerability." NOTE: this issue exists because of an incomplete fix for CVE-2010-2753.
CVE-2015-2713	Use-after-free vulnerability in the SetBreaks function in Mozilla Firefox before 38.0, Firefox ESR 31.x before 31.7, and Thunderbird before 31.7 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via a document containing crafted text in conjunction with a Cascading Style Sheets (CSS) token sequence containing properties related to vertical text.
CVE-2014-1553	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 32.0, Firefox ESR 31.x before 31.1, and Thunderbird 31.x before 31.1 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2003-1330	Clearswift MAILsweeper for SMTP 4.3.6 SP1 does not execute custom "on strip unsuccessful" hooks, which allows remote attackers to bypass e-mail attachment filtering policies via an attachment that MAILsweeper can detect but not remove.
CVE-2008-4564	Stack-based buffer overflow in wp6sr.dll in the Autonomy KeyView SDK 10.4 and earlier, as used in IBM Lotus Notes, Symantec Mail Security (SMS) products, Symantec BrightMail Appliance products, and Symantec Data Loss Prevention (DLP) products, allows remote attackers to execute arbitrary code via a crafted Word Perfect Document (WPD) file.
CVE-2012-3970	Use-after-free vulnerability in the nsTArray_base::Length function in Mozilla Firefox before 15.0, Firefox ESR 10.x before 10.0.7, Thunderbird before 15.0, Thunderbird ESR 10.x before 10.0.7, and SeaMonkey before 2.12 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via vectors involving movement of a requiredFeatures attribute from one SVG document to another.
CVE-2011-3670	Mozilla Firefox before 3.6.26 and 4.x through 6.0, Thunderbird before 3.1.18 and 5.0 through 6.0, and SeaMonkey before 2.4 do not properly enforce the IPv6 literal address syntax, which allows remote attackers to obtain sensitive information by making XMLHttpRequest calls through a proxy and reading the error messages.
CVE-2007-2868	Multiple vulnerabilities in the JavaScript engine for Mozilla Firefox 1.5.x before 1.5.0.12 and 2.x before 2.0.0.4, Thunderbird 1.5.x before 1.5.0.12 and 2.x before 2.0.0.4, and SeaMonkey 1.0.9 and 1.1.2 allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via vectors that trigger memory corruption.
CVE-2013-0770	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 18.0, Thunderbird before 17.0.2, and SeaMonkey before 2.15 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2011-2365	Unspecified vulnerability in the browser engine in Mozilla Firefox 3.6.x before 3.6.18 and Thunderbird before 3.1.11 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors, a different vulnerability than CVE-2011-2364.
CVE-	Heap-based buffer overflow in the nsSaveAsCharset::DoCharsetConversion function in Mozilla Firefox before 19.0, Firefox ESR 17.x

2013-0782	before 17.0.3, Thunderbird before 17.0.3, Thunderbird ESR 17.x before 17.0.3, and SeaMonkey before 2.16 allows remote attackers to execute arbitrary code via unspecified vectors.
CVE-2012-4208	The XrayWrapper implementation in Mozilla Firefox before 17.0, Thunderbird before 17.0, and SeaMonkey before 2.14 does not consider the compartment during property filtering, which allows remote attackers to bypass intended chrome-only restrictions on reading DOM object properties via a crafted web site.
CVE-2010-3778	Unspecified vulnerability in Mozilla Firefox 3.5.x before 3.5.16, Thunderbird before 3.0.11, and SeaMonkey before 2.0.11 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2013-0745	The AutoWrapperChanger class in Mozilla Firefox before 18.0, Firefox ESR 17.x before 17.0.2, Thunderbird before 17.0.2, Thunderbird ESR 17.x before 17.0.2, and SeaMonkey before 2.15 does not properly interact with garbage collection, which allows remote attackers to execute arbitrary code via a crafted HTML document referencing JavaScript objects.
CVE-2007-1792	libdayzero.dll in the Filter Hub Service (filter-hub.exe) in Symantec Mail Security for SMTP before 5.0.1 Patch 181 and Mail Security Appliance before 5.0.0-36 allows remote attackers to cause a denial of service (crash) via a crafted executable attachment in an e-mail, involving the detection of "PE-Shield v0.2" and "ASPack v1.00-1.08.02".
CVE-2013-1675	Mozilla Firefox before 21.0, Firefox ESR 17.x before 17.0.6, Thunderbird before 17.0.6, and Thunderbird ESR 17.x before 17.0.6 do not properly initialize data structures for the nsDOMSVGZoomEvent::mPreviousScale and nsDOMSVGZoomEvent::mNewScale functions, which allows remote attackers to obtain sensitive information from process memory via a crafted web site.
CVE-2016-1961	Use-after-free vulnerability in the nsHTMLDocument::SetBody function in dom/html/nsHTMLDocument.cpp in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7 allows remote attackers to execute arbitrary code by leveraging mishandling of a root element, aka ZDI-CAN-3574.
CVE-2011-2982	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 3.6.20, Thunderbird 2.x and 3.x before 3.1.12, SeaMonkey 1.x and 2.x, and possibly other products allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2004-0765	The cert_TestHostName function in Mozilla before 1.7, Firefox before 0.9, and Thunderbird before 0.7, only checks the hostname portion of a certificate when the hostname portion of the URI is not a fully qualified domain name (FQDN), which allows remote attackers to spoof trusted certificates.
CVE-2015-2725	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 39.0, Firefox ESR 38.x before 38.1, and Thunderbird before 38.1 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2014-1568	Mozilla Network Security Services (NSS) before 3.16.2.1, 3.16.x before 3.16.5, and 3.17.x before 3.17.1, as used in Mozilla Firefox before 32.0.3, Mozilla Firefox ESR 24.x before 24.8.1 and 31.x before 31.1.1, Mozilla Thunderbird before 24.8.1 and 31.x before 31.1.2, Mozilla SeaMonkey before 2.29.1, Google Chrome before 37.0.2062.124 on Windows and OS X, and Google Chrome OS before 37.0.2062.120, does not properly parse ASN.1 values in X.509 certificates, which makes it easier for remote attackers to spoof RSA signatures via a crafted certificate, aka a "signature malleability" issue.
CVE-2011-3647	The JSSubScriptLoader in Mozilla Firefox before 3.6.24 and Thunderbird before 3.1.6 does not properly handle XPCNativeWrappers during calls to the loadSubScript method in an add-on, which makes it easier for remote attackers to gain privileges via a crafted web site that leverages certain unwrapping behavior, a related issue to CVE-2011-3004.
CVE-2011-0069	Unspecified vulnerability in the browser engine in Mozilla Firefox 3.5.x before 3.5.19, 3.6.x before 3.6.17, and 4.x before 4.0.1; Thunderbird before 3.1.10; and SeaMonkey before 2.0.14 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors, a different vulnerability than CVE-2011-0070.
CVE-2004-2417	Format string vulnerability in smtp.c for smtp.proxy 1.1.3 and earlier allows remote attackers to execute arbitrary code via format string specifiers in the (1) client hostname or (2) message-id, which are injected into a syslog message.
CVE-2013-1674	Use-after-free vulnerability in Mozilla Firefox before 21.0, Firefox ESR 17.x before 17.0.6, Thunderbird before 17.0.6, and Thunderbird ESR 17.x before 17.0.6 allows remote attackers to execute arbitrary code via vectors involving an onresize event during the playing of a video.
CVE-2010-1202	Multiple unspecified vulnerabilities in the JavaScript engine in Mozilla Firefox 3.5.x before 3.5.10 and 3.6.x before 3.6.4, Thunderbird before 3.0.5, and SeaMonkey before 2.0.5 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2008-6961	mailnews in Mozilla Thunderbird before 2.0.0.18 and SeaMonkey before 1.1.13, when JavaScript is enabled in mail, allows remote attackers to obtain sensitive information about the recipient, or comments in forwarded mail, via script that reads the (1) .documentURI or (2) .textContent DOM properties.
CVE-2013-1676	The SelectionIterator::GetNextSegment function in Mozilla Firefox before 21.0, Firefox ESR 17.x before 17.0.6, Thunderbird before 17.0.6, and Thunderbird ESR 17.x before 17.0.6 allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2006-0447	Multiple buffer overflows in E-Post Mail Server 4.10 and SPA-PRO Mail @Solomon 4.00 allow remote attackers to execute arbitrary code via a long username to the (1) AUTH PLAIN or (2) AUTH LOGIN SMTP commands, which is not properly handled by (a) EPSTRS.EXE or (b) SPA-RS.EXE; (3) a long username in the APOP POP3 command, which is not properly handled by (c) EPSTPOP4S.EXE or (d) SPA-POP3S.EXE; (4) a long IMAP DELETE command, which is not properly handled by (e) EPSTIMAP4S.EXE or (f) SPA-IMAP4S.EXE.
CVE-2014-1556	Mozilla Firefox before 31.0, Firefox ESR 24.x before 24.7, and Thunderbird before 24.7 allow remote attackers to execute arbitrary code via crafted WebGL content constructed with the Cesium JavaScript library.
CVE-2013-0780	Use-after-free vulnerability in the nsOverflowContinuationTracker::Finish function in Mozilla Firefox before 19.0, Firefox ESR 17.x before 17.0.3, Thunderbird before 17.0.3, Thunderbird ESR 17.x before 17.0.3, and SeaMonkey before 2.16 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via a crafted document that uses Cascading Style Sheets (CSS) -moz-column-* properties.

CVE-2009-3983	Mozilla Firefox before 3.0.16 and 3.5.x before 3.5.6, and SeaMonkey before 2.0.1, allows remote attackers to send authenticated requests to arbitrary applications by replaying the NTLM credentials of a browser user.
CVE-2010-0654	Mozilla Firefox 3.5.x before 3.5.11 and 3.6.x before 3.6.7, Thunderbird 3.0.x before 3.0.6 and 3.1.x before 3.1.1, and SeaMonkey before 2.0.6 permit cross-origin loading of CSS stylesheets even when the stylesheet download has an incorrect MIME type and the stylesheet document is malformed, which allows remote attackers to obtain sensitive information via a crafted document.
CVE-2004-0903	Stack-based buffer overflow in the writeGroup function in nsVCardObj.cpp for Mozilla Firefox before the Preview Release, Mozilla before 1.7.3, and Thunderbird before 0.8 allows remote attackers to execute arbitrary code via malformed VCard attachments that are not properly handled when previewing a message.
CVE-2008-4062	Multiple unspecified vulnerabilities in Mozilla Firefox before 2.0.0.17 and 3.x before 3.0.2, Thunderbird before 2.0.0.17, and SeaMonkey before 1.1.12 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to the JavaScript engine and (1) misinterpretation of the characteristics of Namespace and QName in jsxml.c, (2) misuse of signed integers in the nsEscapeCount function in nsEscape.cpp, and (3) interaction of JavaScript garbage collection with certain use of an NPObject in the nsNPObjWrapper::GetNewOrUsed function in nsJSNPRuntime.cpp.
CVE-2014-1594	Mozilla Firefox before 34.0, Firefox ESR 31.x before 31.3, Thunderbird before 31.3, and SeaMonkey before 2.31 might allow remote attackers to execute arbitrary code by leveraging an incorrect cast from the BasicThebesLayer data type to the BasicContainerLayer data type.
CVE-2009-1304	The JavaScript engine in Mozilla Firefox 3.x before 3.0.9, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.16 allows remote attackers to cause a denial of service (application crash) and possibly trigger memory corruption via vectors involving (1) js_FindPropertyHelper, related to the definitions of Math and Date; and (2) js_CheckRedeclaration.
CVE-2013-1710	The crypto.generateCRMFRequest function in Mozilla Firefox before 23.0, Firefox ESR 17.x before 17.0.8, Thunderbird before 17.0.8, Thunderbird ESR 17.x before 17.0.8, and SeaMonkey before 2.20 allows remote attackers to execute arbitrary JavaScript code or conduct cross-site scripting (XSS) attacks via vectors related to Certificate Request Message Format (CRMF) request generation.
CVE-2012-4181	Use-after-free vulnerability in the nsSMILAnimationController::DoSample function in Mozilla Firefox before 16.0, Firefox ESR 10.x before 10.0.8, Thunderbird before 16.0, Thunderbird ESR 10.x before 10.0.8, and SeaMonkey before 2.13 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2006-1740	Mozilla Firefox 1.x before 1.5 and 1.0.x before 1.0.8, Mozilla Suite before 1.7.13, and SeaMonkey before 1.0 allows remote attackers to spoof secure site indicators such as the locked icon by opening the trusted site in a popup window, then changing the location to a malicious site.
CVE-2006-3812	Mozilla Firefox before 1.5.0.5, Thunderbird before 1.5.0.5, and SeaMonkey before 1.0.3 allows remote attackers to reference remote files and possibly load chrome: URLs by tricking the user into copying or dragging links.
CVE-2012-4209	Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0, Thunderbird ESR 10.x before 10.0.11, and SeaMonkey before 2.14 do not prevent use of a "top" frame name-attribute value to access the location property, which makes it easier for remote attackers to conduct cross-site scripting (XSS) attacks via vectors involving a binary plugin.
CVE-2012-3961	Use-after-free vulnerability in the RangeData implementation in Mozilla Firefox before 15.0, Firefox ESR 10.x before 10.0.7, Thunderbird before 15.0, Thunderbird ESR 10.x before 10.0.7, and SeaMonkey before 2.12 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2010-3167	The nsTreeContentView function in Mozilla Firefox before 3.5.12 and 3.6.x before 3.6.9, Thunderbird before 3.0.7 and 3.1.x before 3.1.3, and SeaMonkey before 2.0.7 does not properly handle node removal in XUL trees, which allows remote attackers to execute arbitrary code via vectors involving access to deleted memory, related to a "dangling pointer vulnerability."
CVE-2006-3811	Multiple vulnerabilities in Mozilla Firefox before 1.5.0.5, Thunderbird before 1.5.0.5, and SeaMonkey before 1.0.3 allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via Javascript that leads to memory corruption, including (1) nsListControlFrame::FireMenuItemActiveEvent, (2) buffer overflows in the string class in out-of-memory conditions, (3) table row and column groups, (4) "anonymous box selectors outside of UA stylesheets," (5) stale references to "removed nodes," and (6) running the crypto.generateCRMFRequest callback on deleted context.
CVE-2009-3984	Mozilla Firefox before 3.0.16 and 3.5.x before 3.5.6, and SeaMonkey before 2.0.1, allows remote attackers to spoof an SSL indicator for an http URL or a file URL by setting document.location to an https URL corresponding to a site that responds with a No Content (aka 204) status code and an empty body.
CVE-2013-0752	Mozilla Firefox before 18.0, Firefox ESR 17.x before 17.0.2, Thunderbird before 17.0.2, Thunderbird ESR 17.x before 17.0.2, and SeaMonkey before 2.15 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XBL file with multiple bindings that have SVG content.
CVE-2010-3166	Heap-based buffer overflow in the nsTextFrameUtils::TransformText function in Mozilla Firefox before 3.5.12 and 3.6.x before 3.6.9, Thunderbird before 3.0.7 and 3.1.x before 3.1.3, and SeaMonkey before 2.0.7 might allow remote attackers to execute arbitrary code via a bidirectional text run.
CVE-2013-1719	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 24.0, Thunderbird before 24.0, and SeaMonkey before 2.21 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2008-5014	jslock.cpp in Mozilla Firefox 3.x before 3.0.2, Firefox 2.x before 2.0.0.18, Thunderbird 2.x before 2.0.0.18, and SeaMonkey 1.x before 1.1.13 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code by modifying the window.__proto__.__proto__ object in a way that causes a lock on a non-native object, which triggers an assertion failure related to the OBJ_IS_NATIVE function.
CVE-2014-1523	Heap-based buffer overflow in the read_u32 function in Mozilla Firefox before 29.0, Firefox ESR 24.x before 24.5, Thunderbird before 24.5, and SeaMonkey before 2.26 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted JPEG image.

CVE-2012-4180	Heap-based buffer overflow in the nsHTMLEditor::IsPrevCharInNodeWhitespace function in Mozilla Firefox before 16.0, Firefox ESR 10.x before 10.0.8, Thunderbird before 16.0, Thunderbird ESR 10.x before 10.0.8, and SeaMonkey before 2.13 allows remote attackers to execute arbitrary code via unspecified vectors.
CVE-2010-1210	intl/uconv/util/nsUnicodeDecodeHelper.cpp in Mozilla Firefox before 3.6.7 and Thunderbird before 3.1.1 inserts a U+FFFD sequence into text in certain circumstances involving undefined positions, which might make it easier for remote attackers to conduct cross-site scripting (XSS) attacks via crafted 8-bit text.
CVE-2013-1709	Mozilla Firefox before 23.0, Firefox ESR 17.x before 17.0.8, Thunderbird before 17.0.8, Thunderbird ESR 17.x before 17.0.8, and SeaMonkey before 2.20 do not properly handle the interaction between FRAME elements and history, which allows remote attackers to conduct cross-site scripting (XSS) attacks via vectors involving spoofing a relative location in a previously visited document.
CVE-2014-1555	Use-after-free vulnerability in the nsDocLoader::OnProgress function in Mozilla Firefox before 31.0, Firefox ESR 24.x before 24.7, and Thunderbird before 24.7 allows remote attackers to execute arbitrary code via vectors that trigger a FireOnStateChange event.
CVE-2009-1303	The browser engine in Mozilla Firefox before 3.0.9, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.16 allows remote attackers to cause a denial of service (application crash) and possibly trigger memory corruption via vectors related to nsSVGElement::BindToTree.
CVE-2001-1542	NAI WebShield SMTP 4.5 and possibly 4.5 MR1a does not filter improperly MIME encoded email attachments, which could allow remote attackers to bypass filtering and possibly execute arbitrary code in email clients that process the invalid attachments.
CVE-2014-1563	Use-after-free vulnerability in the mozilla::DOMSVGLength::GetTearOff function in Mozilla Firefox before 32.0, Firefox ESR 31.x before 31.1, and Thunderbird 31.x before 31.1 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via an SVG animation with DOM interaction that triggers incorrect cycle collection.
CVE-2006-5463	Unspecified vulnerability in Mozilla Firefox before 1.5.0.8, Thunderbird before 1.5.0.8, and SeaMonkey before 1.0.6 allows remote attackers to execute arbitrary JavaScript bytecode via unspecified vectors involving modification of a Script object while it is executing.
CVE-2012-3960	Use-after-free vulnerability in the mozSpellChecker::SetCurrentDictionary function in Mozilla Firefox before 15.0, Firefox ESR 10.x before 10.0.7, Thunderbird before 15.0, Thunderbird ESR 10.x before 10.0.7, and SeaMonkey before 2.12 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2008-4065	Mozilla Firefox before 2.0.0.17 and 3.x before 3.0.2, Thunderbird before 2.0.0.17, and SeaMonkey before 1.1.12 allow remote attackers to bypass cross-site scripting (XSS) protection mechanisms and conduct XSS attacks via byte order mark (BOM) characters that are removed from JavaScript code before execution, aka "Stripped BOM characters bug."
CVE-2013-6673	Mozilla Firefox before 26.0, Firefox ESR 24.x before 24.2, Thunderbird before 24.2, and SeaMonkey before 2.23 do not recognize a user's removal of trust from an EV X.509 certificate, which makes it easier for man-in-the-middle attackers to spoof SSL servers in opportunistic circumstances via a valid certificate that is unacceptable to the user.
CVE-2005-2409	Format string vulnerability in util.c in nbsmtp 0.99 and earlier, while running in debug mode, allows remote attackers to execute arbitrary code via format string specifiers that are not properly handled in a syslog call.
CVE-2010-1211	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 3.5.x before 3.5.11 and 3.6.x before 3.6.7, Thunderbird 3.0.x before 3.0.6 and 3.1.x before 3.1.1, and SeaMonkey before 2.0.6 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2011-0081	Unspecified vulnerability in the browser engine in Mozilla Firefox 3.6.x before 3.6.17 and 4.x before 4.0.1, and Thunderbird 3.1.x before 3.1.10, allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2009-1392	The browser engine in Mozilla Firefox 3 before 3.0.11, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.17 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to (1) nsEventStateManager::GetContentState and nsNativeTheme::CheckBooleanAttr; (2) UnhookTextRunFromFrames and ClearAllTextRunReferences; (3) nsTextFrame::ClearTextRun; (4) IsPercentageAware; (5) PL_DHashTableFinish; (6) nsListBoxBodyFrame::GetNextItemBox; (7) AtomTableClearEntry, related to the atom table, DOM mutation events, and Unicode surrogates; (8) nsHTMLEditor::HideResizers; and (9) nsWindow::SetCursor, related to changing the cursor; and other vectors.
CVE-2016-1954	The nsCSPContext::SendReports function in dom/security/nsCSPContext.cpp in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7 does not prevent use of a non-HTTP report-uri for a Content Security Policy (CSP) violation report, which allows remote attackers to cause a denial of service (data overwrite) or possibly gain privileges by specifying a URL of a local file.
CVE-2011-2371	Integer overflow in the Array.reduceRight method in Mozilla Firefox before 3.6.18 and 4.x through 4.0.1, Thunderbird before 3.1.11, and SeaMonkey through 2.0.14 allows remote attackers to execute arbitrary code via vectors involving a long JavaScript Array object.
CVE-2009-1302	The browser engine in Mozilla Firefox 3.x before 3.0.9, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.16 allows remote attackers to cause a denial of service (application crash) and possibly trigger memory corruption via vectors related to (1) nsAsyncInstantiateEvent::Run, (2) nsStyleContext::Destroy, (3) nsComputedDOMStyle::GetWidth, (4) the xslt_attributeset_ImportSameName.html test case for the XSLT stylesheet compiler, (5) nsXULDocument::SynchronizeBroadcastListener, (6) IsBindingAncestor, (7) PL_DHashTableOperate and nsEditor::EndUpdateViewBatch, and (8) gfxSkipCharsIterator::SetOffsets, and other vectors.
CVE-2013-1677	The gfxSkipCharsIterator::SetOffsets function in Mozilla Firefox before 21.0, Firefox ESR 17.x before 17.0.6, Thunderbird before 17.0.6, and Thunderbird ESR 17.x before 17.0.6 allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2012-0454	Use-after-free vulnerability in Mozilla Firefox 4.x through 10.0, Firefox ESR 10.x before 10.0.3, Thunderbird 5.0 through 10.0, Thunderbird ESR 10.x before 10.0.3, and SeaMonkey before 2.8 on 32-bit Windows 7 platforms allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via vectors involving use of the file-open dialog in a child

	window, related to the IUnknown_QueryService function in the Windows shlwapi.dll library.
CVE-2015-2724	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 39.0, Firefox ESR 31.x before 31.8 and 38.x before 38.1, and Thunderbird before 38.1 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2014-1524	The nsXBLProtoImpl::InstallImplementation function in Mozilla Firefox before 29.0, Firefox ESR 24.x before 24.5, Thunderbird before 24.5, and SeaMonkey before 2.26 does not properly check whether objects are XBL objects, which allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow) via crafted JavaScript code that accesses a non-XBL object as if it were an XBL object.
CVE-2007-1252	Buffer overflow in Symantec Mail Security for SMTP 5.0 before Patch 175 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via crafted headers in an e-mail message. NOTE: some information was obtained from third party sources.
CVE-2010-2770	Mozilla Firefox before 3.5.12 and 3.6.x before 3.6.9, Thunderbird before 3.0.7 and 3.1.x before 3.1.3, and SeaMonkey before 2.0.7 on Mac OS X allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via a crafted font in a data: URL.
CVE-2012-3963	Use-after-free vulnerability in the js::gc::MapAllocToTraceKind function in Mozilla Firefox before 15.0, Firefox ESR 10.x before 10.0.7, Thunderbird before 15.0, Thunderbird ESR 10.x before 10.0.7, and SeaMonkey before 2.12 allows remote attackers to execute arbitrary code via unspecified vectors.
CVE-2012-5830	Use-after-free vulnerability in Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0, Thunderbird ESR 10.x before 10.0.11, and SeaMonkey before 2.14 on Mac OS X allows remote attackers to execute arbitrary code via an HTML document.
CVE-2010-1213	The importScripts Web Worker method in Mozilla Firefox 3.5.x before 3.5.11 and 3.6.x before 3.6.7, Thunderbird 3.0.x before 3.0.6 and 3.1.x before 3.1.1, and SeaMonkey before 2.0.6 does not verify that content is valid JavaScript code, which allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via a crafted HTML document.
CVE-2009-0776	nsIRDFService in Mozilla Firefox before 3.0.7, Thunderbird before 2.0.0.21, and SeaMonkey before 1.1.15 allows remote attackers to bypass the same-origin policy and read XML data from another domain via a cross-domain redirect.
CVE-2010-1200	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 3.5.x before 3.5.10 and 3.6.x before 3.6.4, Thunderbird before 3.0.5, and SeaMonkey before 2.0.5 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2013-1679	Use-after-free vulnerability in the mozilla::plugins::child::_geturlnotify function in Mozilla Firefox before 21.0, Firefox ESR 17.x before 17.0.6, Thunderbird before 17.0.6, and Thunderbird ESR 17.x before 17.0.6 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2008-1235	Unspecified vulnerability in Mozilla Firefox before 2.0.0.13, Thunderbird before 2.0.0.13, and SeaMonkey before 1.1.9 allows remote attackers to execute arbitrary code via unknown vectors that cause JavaScript to execute with the wrong principal, aka "Privilege escalation via incorrect principals."
CVE-2013-0753	Use-after-free vulnerability in the serializeToStream implementation in the XMLSerializer component in Mozilla Firefox before 18.0, Firefox ESR 10.x before 10.0.12 and 17.x before 17.0.2, Thunderbird before 17.0.2, Thunderbird ESR 10.x before 10.0.12 and 17.x before 17.0.2, and SeaMonkey before 2.15 allows remote attackers to execute arbitrary code via crafted web content.
CVE-2013-1713	Mozilla Firefox before 23.0, Firefox ESR 17.x before 17.0.8, Thunderbird before 17.0.8, Thunderbird ESR 17.x before 17.0.8, and SeaMonkey before 2.20 use an incorrect URI within unspecified comparisons during enforcement of the Same Origin Policy, which allows remote attackers to conduct cross-site scripting (XSS) attacks or install arbitrary add-ons via a crafted web site.
CVE-2010-3175	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 3.6.x before 3.6.11 and Thunderbird 3.1.x before 3.1.5 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2008-5016	The layout engine in Mozilla Firefox 3.x before 3.0.4, Thunderbird 2.x before 2.0.0.18, and SeaMonkey 1.x before 1.1.13 allows remote attackers to cause a denial of service (crash) via multiple vectors that trigger an assertion failure or other consequences.
CVE-2014-1562	Unspecified vulnerability in the browser engine in Mozilla Firefox before 32.0, Firefox ESR 24.x before 24.8 and 31.x before 31.1, and Thunderbird 24.x before 24.8 and 31.x before 31.1 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2013-0778	The ClusterIterator::NextCluster function in Mozilla Firefox before 19.0, Thunderbird before 17.0.3, and SeaMonkey before 2.16 allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2015-2738	The YCbCrImageDataDeserializer::ToDataSourceSurface function in the YCbCr implementation in Mozilla Firefox before 39.0, Firefox ESR 31.x before 31.8 and 38.x before 38.1, and Thunderbird before 38.1 reads data from uninitialized memory locations, which has unspecified impact and attack vectors.
CVE-2006-2779	Mozilla Firefox and Thunderbird before 1.5.0.4 allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via (1) nested <option> tags in a select tag, (2) a DOMNodeRemoved mutation event, (3) "Content-implemented tree views," (4) BoxObjects, (5) the XBL implementation, (6) an iframe that attempts to remove itself, which leads to memory corruption.
CVE-2013-0787	Use-after-free vulnerability in the nsEditor::IsPreformatted function in editor/libeditor/base/nsEditor.cpp in Mozilla Firefox before 19.0.2, Firefox ESR 17.x before 17.0.4, Thunderbird before 17.0.4, Thunderbird ESR 17.x before 17.0.4, and SeaMonkey before 2.16.1 allows remote attackers to execute arbitrary code via vectors involving an execCommand call.
CVE-2013-	The _cairo_xlib_surface_add_glyph function in Mozilla Firefox before 21.0, Firefox ESR 17.x before 17.0.6, Thunderbird before 17.0.6, and Thunderbird ESR 17.x before 17.0.6 allows remote attackers to execute arbitrary code or cause a denial of service (invalid write

1678	operation) via unspecified vectors.
CVE-2011-3005	Use-after-free vulnerability in Mozilla Firefox 4.x through 6, Thunderbird before 7.0, and SeaMonkey before 2.4 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via crafted OGG headers in a .ogg file.
CVE-2007-3796	The password reset feature in the Spam Quarantine HTTP interface for MailMarshal SMTP 6.2.0.x before 6.2.1 allows remote attackers to modify arbitrary account information via a UserId variable with a large amount of trailing whitespace followed by a malicious value, which triggers SQL buffer truncation due to length inconsistencies between variables.
CVE-2010-5074	The layout engine in Mozilla Firefox before 4.0, Thunderbird before 3.3, and SeaMonkey before 2.1 executes different code for visited and unvisited links during the processing of Cascading Style Sheets (CSS) token sequences, which makes it easier for remote attackers to obtain sensitive information about visited web pages via a timing attack.
CVE-2011-0080	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 3.5.x before 3.5.19 and 3.6.x before 3.6.17, Thunderbird before 3.1.10, and SeaMonkey before 2.0.14 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2009-0777	Mozilla Firefox before 3.0.7, Thunderbird before 2.0.0.21, and SeaMonkey before 1.1.15 decode invisible characters when they are displayed in the location bar, which causes an incorrect address to be displayed and makes it easier for remote attackers to spoof URLs and conduct phishing attacks.
CVE-2009-1307	The view-source: URI implementation in Mozilla Firefox before 3.0.9, Thunderbird, and SeaMonkey does not properly implement the Same Origin Policy, which allows remote attackers to (1) bypass crossdomain.xml restrictions and connect to arbitrary web sites via a Flash file; (2) read, create, or modify Local Shared Objects via a Flash file; or (3) bypass unspecified restrictions and render content via vectors involving a jar: URI.
CVE-2013-0779	The nsCodingStateMachine::NextState function in Mozilla Firefox before 19.0, Thunderbird before 17.0.3, and SeaMonkey before 2.16 allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2008-5017	Integer overflow in xpcom/io/nsEscape.cpp in the browser engine in Mozilla Firefox 3.x before 3.0.4, Firefox 2.x before 2.0.0.18, Thunderbird 2.x before 2.0.0.18, and SeaMonkey 1.x before 1.1.13 allows remote attackers to cause a denial of service (crash) via unknown vectors.
CVE-2008-4067	Directory traversal vulnerability in Mozilla Firefox before 2.0.0.17 and 3.x before 3.0.2, Thunderbird before 2.0.0.17, and SeaMonkey before 1.1.12 on Linux allows remote attackers to read arbitrary files via a .. (dot dot) and URL-encoded / (slash) characters in a resource: URI.
CVE-2012-3962	Mozilla Firefox before 15.0, Firefox ESR 10.x before 10.0.7, Thunderbird before 15.0, Thunderbird ESR 10.x before 10.0.7, and SeaMonkey before 2.12 do not properly iterate through the characters in a text run, which allows remote attackers to execute arbitrary code via a crafted document.
CVE-2010-1212	js/src/jstracer.cpp in the browser engine in Mozilla Firefox 3.6.x before 3.6.7 and Thunderbird 3.1.x before 3.1.1 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to (1) propagation of deep aborts in the TraceRecorder::record_JSOP_BINDNAME function, (2) depth handling in the TraceRecorder::record_JSOP_GETELEM function, and (3) tracing of out-of-range arguments in the TraceRecorder::record_JSOP_ARGSUB function.
CVE-2011-3079	The Inter-process Communication (IPC) implementation in Google Chrome before 18.0.1025.168, as used in Mozilla Firefox before 38.0 and other products, does not properly validate messages, which has unspecified impact and attack vectors.
CVE-2013-1712	Multiple untrusted search path vulnerabilities in updater.exe in Mozilla Updater in Mozilla Firefox before 23.0, Firefox ESR 17.x before 17.0.8, Thunderbird before 17.0.8, and Thunderbird ESR 17.x before 17.0.8 on Windows 7, Windows Server 2008 R2, Windows 8, and Windows Server 2012 allow local users to gain privileges via a Trojan horse DLL in (1) the update directory or (2) the current working directory.
CVE-2012-5829	Heap-based buffer overflow in the nsWindow::OnExposeEvent function in Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0, Thunderbird ESR 10.x before 10.0.11, and SeaMonkey before 2.14 allows remote attackers to execute arbitrary code via unspecified vectors.
CVE-2009-0774	The layout engine in Mozilla Firefox 2 and 3 before 3.0.7, Thunderbird before 2.0.0.21, and SeaMonkey 1.1.15 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via vectors related to gczeal, a different vulnerability than CVE-2009-0773.
CVE-2010-1201	Unspecified vulnerability in the browser engine in Mozilla Firefox 3.5.x before 3.5.10, Thunderbird before 3.0.5, and SeaMonkey before 2.0.5 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2009-1306	The jar: URI implementation in Mozilla Firefox before 3.0.9, Thunderbird, and SeaMonkey does not follow the Content-Disposition header of the inner URI, which allows remote attackers to conduct cross-site scripting (XSS) attacks and possibly other attacks via an uploaded .jar file with a "Content-Disposition: attachment" designation.
CVE-2004-1312	A bug in the HTML parser in a certain Microsoft HTML library, as used in various third party products, may allow remote attackers to cause a denial of service via certain strings, as reported in GFI MailEssentials for Exchange 9 and 10, and GFI MailSecurity for Exchange 8, which causes emails to remain in IIS or Exchange mail queues.
CVE-2013-0754	Use-after-free vulnerability in the ListenerManager implementation in Mozilla Firefox before 18.0, Firefox ESR 10.x before 10.0.12 and 17.x before 17.0.2, Thunderbird before 17.0.2, Thunderbird ESR 10.x before 10.0.12 and 17.x before 17.0.2, and SeaMonkey before 2.15 allows remote attackers to execute arbitrary code via vectors involving the triggering of garbage collection after memory allocation for listener objects.
CVE-2010-	Cross-site scripting (XSS) vulnerability in Mozilla Firefox before 3.5.12 and 3.6.x before 3.6.9, Thunderbird before 3.0.7 and 3.1.x before 3.1.3, and SeaMonkey before 2.0.7 allows user-assisted remote attackers to inject arbitrary web script or HTML via a selection that is

2769	added to a document in which the designMode property is enabled.
CVE-2008-4068	Directory traversal vulnerability in Mozilla Firefox before 2.0.0.17 and 3.x before 3.0.2, Thunderbird before 2.0.0.17, and SeaMonkey before 1.1.12 allows remote attackers to bypass "restrictions imposed on local HTML files," and obtain sensitive information and prompt users to write this information into a file, via directory traversal sequences in a resource: URI.
CVE-2012-4179	Use-after-free vulnerability in the nsHTMLCSSUtils::CreateCSSPropertyTxn function in Mozilla Firefox before 16.0, Firefox ESR 10.x before 10.0.8, Thunderbird before 16.0, Thunderbird ESR 10.x before 10.0.8, and SeaMonkey before 2.13 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2013-1680	Use-after-free vulnerability in the nsFrameList::FirstChild function in Mozilla Firefox before 21.0, Firefox ESR 17.x before 17.0.6, Thunderbird before 17.0.6, and Thunderbird ESR 17.x before 17.0.6 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2005-3402	The SMTP client in Mozilla Thunderbird 1.0.5 BETA, 1.0.7, and possibly other versions, does not notify users when it cannot establish a secure channel with the server, which allows remote attackers to obtain authentication information without detection via a man-in-the-middle (MITM) attack that bypasses TLS authentication or downgrades CRAM-MD5 authentication to plain authentication.
CVE-2014-1557	The ConvolveHorizontally function in Skia, as used in Mozilla Firefox before 31.0, Firefox ESR 24.x before 24.7, and Thunderbird before 24.7, does not properly handle the discarding of image data during function execution, which allows remote attackers to execute arbitrary code by triggering prolonged image scaling, as demonstrated by scaling of a high-quality image.
CVE-2009-0775	Double free vulnerability in Mozilla Firefox before 3.0.7, Thunderbird before 2.0.0.21, and SeaMonkey before 1.1.15 allows remote attackers to execute arbitrary code via "cloned XUL DOM elements which were linked as a parent and child," which are not properly handled during garbage collection.
CVE-2014-1574	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 33.0, Firefox ESR 31.x before 31.2, and Thunderbird 31.x before 31.2 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2009-1305	The JavaScript engine in Mozilla Firefox before 3.0.9, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.16 allows remote attackers to cause a denial of service (application crash) and possibly trigger memory corruption via vectors involving JSOP_DEFVAR and properties that lack the JSPROP_PERMANENT attribute.
CVE-2008-4070	Heap-based buffer overflow in Mozilla Thunderbird before 2.0.0.17 and SeaMonkey before 1.1.12 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a long header in a news article, related to "canceling [a] newsgroup message" and "cancelled newsgroup messages."
CVE-2002-1090	Buffer overflow in read_smtp_response of protocol.c in libesmtp before 0.8.11 allows a remote SMTP server to (1) execute arbitrary code via a certain response or (2) cause a denial of service via long server responses.
CVE-2004-1291	Buffer overflow in qwik-smtpd allows remote attackers to use the server as an SMTP spam relay via a long HELO command, which overwrites the adjacent localIP data buffer.
CVE-2013-1717	Mozilla Firefox before 23.0, Firefox ESR 17.x before 17.0.8, Thunderbird before 17.0.8, Thunderbird ESR 17.x before 17.0.8, and SeaMonkey before 2.20 do not properly restrict local-filesystem access by Java applets, which allows user-assisted remote attackers to read arbitrary files by leveraging a download to a fixed pathname or other predictable pathname.
CVE-2013-0777	Use-after-free vulnerability in the nsDisplayBoxShadowOuter::Paint function in Mozilla Firefox before 19.0, Thunderbird before 17.0.3, and SeaMonkey before 2.16 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2009-2463	Multiple integer overflows in the (1) PL_Base64Decode and (2) PL_Base64Encode functions in nsprpub/lib/libc/src/base64.c in Mozilla Firefox before 3.0.12, Thunderbird before 2.0.0.24, and SeaMonkey before 1.1.19 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unspecified vectors that trigger buffer overflows.
CVE-2011-3001	Mozilla Firefox 4.x through 6, Thunderbird before 7.0, and SeaMonkey before 2.4 do not prevent manual add-on installation in response to the holding of the Enter key, which allows user-assisted remote attackers to bypass intended access restrictions via a crafted web site that triggers an unspecified internal error.
CVE-2014-1551	Use-after-free vulnerability in the FontTableRec destructor in Mozilla Firefox before 31.0, Firefox ESR 24.x before 24.7, and Thunderbird before 24.7 on Windows allows remote attackers to execute arbitrary code via crafted use of fonts in MathML content, leading to improper handling of a DirectWrite font-face object.
CVE-2013-6674	Cross-site scripting (XSS) vulnerability in Mozilla Thunderbird 17.x through 17.0.8, Thunderbird ESR 17.x through 17.0.10, and SeaMonkey before 2.20 allows user-assisted remote attackers to inject arbitrary web script or HTML via an e-mail message containing a data: URL in an IFRAME element, a related issue to CVE-2014-2018.
CVE-2012-5833	The texImage2D implementation in the WebGL subsystem in Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0, Thunderbird ESR 10.x before 10.0.11, and SeaMonkey before 2.14 does not properly interact with Mesa drivers, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via function calls involving certain values of the level parameter.
CVE-2009-0353	Unspecified vulnerability in Mozilla Firefox 3.x before 3.0.6, Thunderbird before 2.0.0.21, and SeaMonkey before 1.1.15 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to the JavaScript engine.
CVE-2009-2210	Mozilla Thunderbird before 2.0.0.22 and SeaMonkey before 1.1.17 allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a multipart/alternative e-mail message containing a text/enhanced part that triggers access to an incorrect object type.
CVE-2010-1215	Mozilla Firefox 3.6.x before 3.6.7 and Thunderbird 3.1.x before 3.1.1 do not properly implement access to a content object through a SafeJSObjectWrapper (aka SJOW) wrapper, which allows remote attackers to execute arbitrary JavaScript code with chrome privileges by leveraging "access to an object from the chrome scope."

CVE-2012-0479	Mozilla Firefox 4.x through 11.0, Firefox ESR 10.x before 10.0.4, Thunderbird 5.0 through 11.0, Thunderbird ESR 10.x before 10.0.4, and SeaMonkey before 2.9 allow remote attackers to spoof the address bar via an https URL for invalid (1) RSS or (2) Atom XML content.
CVE-2014-1576	Heap-based buffer overflow in the nsTransformedTextRun function in Mozilla Firefox before 33.0, Firefox ESR 31.x before 31.2, and Thunderbird 31.x before 31.2 allows remote attackers to execute arbitrary code via Cascading Style Sheets (CSS) token sequences that trigger changes to capitalization style.
CVE-2009-0652	The Internationalized Domain Names (IDN) blacklist in Mozilla Firefox 3.0.6 and other versions before 3.0.9; Thunderbird before 2.0.0.21; and SeaMonkey before 1.1.15 does not include box-drawing characters, which allows remote attackers to spoof URLs and conduct phishing attacks, as demonstrated by homoglyphs of the / (slash) and ? (question mark) characters in a subdomain of a .cn domain name, a different vulnerability than CVE-2005-0233. NOTE: some third parties claim that 3.0.6 is not affected, but much older versions perhaps are affected.
CVE-2011-2366	Mozilla Gecko before 5.0, as used in Firefox before 5.0 and Thunderbird before 5.0, does not block use of a cross-domain image as a WebGL texture, which allows remote attackers to obtain approximate copies of arbitrary images via a timing attack involving a crafted WebGL fragment shader.
CVE-2012-0451	CRLF injection vulnerability in Mozilla Firefox 4.x through 10.0, Firefox ESR 10.x before 10.0.3, Thunderbird 5.0 through 10.0, Thunderbird ESR 10.x before 10.0.3, and SeaMonkey before 2.8 allows remote web servers to bypass intended Content Security Policy (CSP) restrictions and possibly conduct cross-site scripting (XSS) attacks via crafted HTTP headers.
CVE-2012-3995	The IsCSSWordSpacingSpace function in Mozilla Firefox before 16.0, Firefox ESR 10.x before 10.0.8, Thunderbird before 16.0, Thunderbird ESR 10.x before 10.0.8, and SeaMonkey before 2.13 allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2010-2768	Mozilla Firefox before 3.5.12 and 3.6.x before 3.6.9, Thunderbird before 3.0.7 and 3.1.x before 3.1.3, and SeaMonkey before 2.0.7 do not properly restrict use of the type attribute of an OBJECT element to set a document's charset, which allows remote attackers to bypass cross-site scripting (XSS) protection mechanisms via UTF-7 encoding.
CVE-2012-0449	Mozilla Firefox before 3.6.26 and 4.x through 9.0, Thunderbird before 3.1.18 and 5.0 through 9.0, and SeaMonkey before 2.7 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via a malformed XSLT stylesheet that is embedded in a document.
CVE-2012-3964	Use-after-free vulnerability in the gfxTextRun::GetUserData function in Mozilla Firefox before 15.0, Firefox ESR 10.x before 10.0.7, Thunderbird before 15.0, Thunderbird ESR 10.x before 10.0.7, and SeaMonkey before 2.12 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2014-1587	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 34.0, Firefox ESR 31.x before 31.3, Thunderbird before 31.3, and SeaMonkey before 2.31 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2014-1592	Use-after-free vulnerability in the nsHtml5TreeOperation function in xul.dll in Mozilla Firefox before 34.0, Firefox ESR 31.x before 31.3, Thunderbird before 31.3, and SeaMonkey before 2.31 allows remote attackers to execute arbitrary code by adding a second root element to an HTML5 document during parsing.
CVE-2014-8639	Mozilla Firefox before 35.0, Firefox ESR 31.x before 31.4, Thunderbird before 31.4, and SeaMonkey before 2.32 do not properly interpret Set-Cookie headers within responses that have a 407 (aka Proxy Authentication Required) status code, which allows remote HTTP proxy servers to conduct session fixation attacks by providing a cookie name that corresponds to the session cookie of the origin server.
CVE-2013-1681	Use-after-free vulnerability in the nsContentUtils::RemoveScriptBlocker function in Mozilla Firefox before 21.0, Firefox ESR 17.x before 17.0.6, Thunderbird before 17.0.6, and Thunderbird ESR 17.x before 17.0.6 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2008-0304	Heap-based buffer overflow in Mozilla Thunderbird before 2.0.0.12 and SeaMonkey before 1.1.8 might allow remote attackers to execute arbitrary code via a crafted external-body MIME type in an e-mail message, related to an incorrect memory allocation during message preview.
CVE-2009-1309	Mozilla Firefox before 3.0.9, Thunderbird, and SeaMonkey do not properly implement the Same Origin Policy for (1) XMLHttpRequest, involving a mismatch for a document's principal, and (2) XPCNativeWrapper.toString, involving an incorrect __proto__ scope, which allows remote attackers to conduct cross-site scripting (XSS) attacks and possibly other attacks via a crafted document.
CVE-2012-4212	Use-after-free vulnerability in the XPCWrappedNative::Mark function in Mozilla Firefox before 17.0, Thunderbird before 17.0, and SeaMonkey before 2.14 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2009-2464	The nsXULTemplateQueryProcessorRDF::CheckIsSeparator function in Mozilla Firefox before 3.0.12, SeaMonkey 2.0a1pre, and Thunderbird allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to loading multiple RDF files in a XUL tree element.
CVE-2011-0078	Unspecified vulnerability in the browser engine in Mozilla Firefox 3.5.x before 3.5.19 and 3.6.x before 3.6.17, Thunderbird before 3.1.10, and SeaMonkey before 2.0.14 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors, a different vulnerability than CVE-2011-0072, CVE-2011-0074, CVE-2011-0075, and CVE-2011-0077.
CVE-2011-2375	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 5.0 and Thunderbird through 3.1.11 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2013-0749	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 18.0, Firefox ESR 17.x before 17.0.1, Thunderbird before 17.0.2, Thunderbird ESR 17.x before 17.0.1, and SeaMonkey before 2.15 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2010-	Integer overflow in the XSLT node sorting implementation in Mozilla Firefox 3.5.x before 3.5.10 and 3.6.x before 3.6.4, Thunderbird before 3.0.5, and SeaMonkey before 2.0.5 allows remote attackers to execute arbitrary code via a large text value for a node.

1199	
CVE-2009-1308	Cross-site scripting (XSS) vulnerability in Mozilla Firefox before 3.0.9, Thunderbird, and SeaMonkey allows remote attackers to inject arbitrary web script or HTML via vectors involving XBL JavaScript bindings and remote stylesheets, as exploited in the wild by a March 2009 eBay listing.
CVE-2006-0836	Mozilla Thunderbird 1.5 allows user-assisted attackers to cause an unspecified denial of service by tricking the user into importing an LDIF file with a long field into the address book, as demonstrated by a long homePhone field.
CVE-2012-0447	Mozilla Firefox 4.x through 9.0, Thunderbird 5.0 through 9.0, and SeaMonkey before 2.7 do not properly initialize data for image/vnd.microsoft.icon images, which allows remote attackers to obtain potentially sensitive information by reading a PNG image that was created through conversion from an ICO image.
CVE-2006-5551	Stack-based buffer overflow in QK SMTP 3.01 and earlier might allow remote attackers to execute arbitrary code via a long argument to the RCPT TO command.
CVE-2012-1967	Mozilla Firefox 4.x through 13.0, Firefox ESR 10.x before 10.0.6, Thunderbird 5.0 through 13.0, Thunderbird ESR 10.x before 10.0.6, and SeaMonkey before 2.11 do not properly implement the JavaScript sandbox utility, which allows remote attackers to execute arbitrary JavaScript code with improper privileges via a javascript: URL.
CVE-2012-3994	Mozilla Firefox before 16.0, Firefox ESR 10.x before 10.0.8, Thunderbird before 16.0, Thunderbird ESR 10.x before 10.0.8, and SeaMonkey before 2.13 allow remote attackers to conduct cross-site scripting (XSS) attacks via a binary plugin that uses Object.defineProperty to shadow the top object, and leverages the relationship between top.location and the location property.
CVE-2009-3980	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 3.5.x before 3.5.6, SeaMonkey before 2.0.1, and Thunderbird allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2012-0441	The ASN.1 decoder in the QuickDER decoder in Mozilla Network Security Services (NSS) before 3.13.4, as used in Firefox 4.x through 12.0, Firefox ESR 10.x before 10.0.5, Thunderbird 5.0 through 12.0, Thunderbird ESR 10.x before 10.0.5, and SeaMonkey before 2.10, allows remote attackers to cause a denial of service (application crash) via a zero-length item, as demonstrated by (1) a zero-length basic constraint or (2) a zero-length field in an OCSP response.
CVE-2013-1714	The Web Workers implementation in Mozilla Firefox before 23.0, Firefox ESR 17.x before 17.0.8, Thunderbird before 17.0.8, Thunderbird ESR 17.x before 17.0.8, and SeaMonkey before 2.20 does not properly restrict XMLHttpRequest calls, which allows remote attackers to bypass the Same Origin Policy and conduct cross-site scripting (XSS) attacks via unspecified vectors.
CVE-2008-1380	The JavaScript engine in Mozilla Firefox before 2.0.0.14, Thunderbird before 2.0.0.14, and SeaMonkey before 1.1.10 allows remote attackers to cause a denial of service (garbage collector crash) and possibly have other impacts via a crafted web page. NOTE: this is due to an incorrect fix for CVE-2008-1237.
CVE-2009-3981	Unspecified vulnerability in the browser engine in Mozilla Firefox before 3.0.16, SeaMonkey before 2.0.1, and Thunderbird allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2014-1565	The mozilla::dom::AudioEventTimeline function in the Web Audio API implementation in Mozilla Firefox before 32.0, Firefox ESR 31.x before 31.1, and Thunderbird 31.x before 31.1 does not properly create audio timelines, which allows remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via crafted API calls.
CVE-2014-1595	Mozilla Firefox before 34.0, Firefox ESR 31.x before 31.3, and Thunderbird before 31.3 on Apple OS X 10.10 omit a CoreGraphics disable-logging action that is needed by jemalloc-based applications, which allows local users to obtain sensitive information by reading /tmp files, as demonstrated by credential information.
CVE-2011-0077	Unspecified vulnerability in the browser engine in Mozilla Firefox 3.5.x before 3.5.19 and 3.6.x before 3.6.17, Thunderbird before 3.1.10, and SeaMonkey before 2.0.14 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors, a different vulnerability than CVE-2011-0072, CVE-2011-0074, CVE-2011-0075, and CVE-2011-0078.
CVE-2010-2767	The navigator.plugins implementation in Mozilla Firefox before 3.5.12 and 3.6.x before 3.6.9, Thunderbird before 3.0.7 and 3.1.x before 3.1.3, and SeaMonkey before 2.0.7 does not properly handle destruction of the DOM plugin array, which might allow remote attackers to cause a denial of service (application crash) or execute arbitrary code via crafted access to the navigator object, related to a "dangling pointer vulnerability."
CVE-2008-1438	Unspecified vulnerability in Microsoft Malware Protection Engine (mpengine.dll) 1.1.3520.0 and 0.1.13.192, as used in multiple Microsoft products, allows context-dependent attackers to cause a denial of service (disk space exhaustion) via a file with "crafted data structures" that trigger the creation of large temporary files, a different vulnerability than CVE-2008-1437.
CVE-2015-2731	Use-after-free vulnerability in the CSPService::ShouldLoad function in the microtask implementation in Mozilla Firefox before 39.0, Firefox ESR 38.x before 38.1, and Thunderbird before 38.1 allows remote attackers to execute arbitrary code by leveraging client-side JavaScript that triggers removal of a DOM object on the basis of a Content Policy.
CVE-2012-3993	The Chrome Object Wrapper (COW) implementation in Mozilla Firefox before 16.0, Firefox ESR 10.x before 10.0.8, Thunderbird before 16.0, Thunderbird ESR 10.x before 10.0.8, and SeaMonkey before 2.13 does not properly interact with failures of InstallTrigger methods, which allows remote attackers to execute arbitrary JavaScript code with chrome privileges via a crafted web site, related to an "XrayWrapper pollution" issue.
CVE-2014-1529	The Web Notification API in Mozilla Firefox before 29.0, Firefox ESR 24.x before 24.5, Thunderbird before 24.5, and SeaMonkey before 2.26 allows remote attackers to bypass intended source-component restrictions and execute arbitrary JavaScript code in a privileged context via a crafted web page for which Notification.permission is granted.
CVE-2016-1957	Memory leak in libstagefright in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7 allows remote attackers to cause a denial of service (memory consumption) via an MPEG-4 file that triggers a delete operation on an array.

CVE-2011-3671	Use-after-free vulnerability in the nsHTMLSelectElement function in nsHTMLSelectElement.cpp in Mozilla Firefox 4.x through 8.0, Thunderbird 5.0 through 8.0, and SeaMonkey before 2.6 allows remote attackers to execute arbitrary code via vectors involving removal of the parent node of an element.
CVE-2006-0299	The E4X implementation in Mozilla Firefox before 1.5.0.1, Thunderbird 1.5 if running Javascript in mail, and SeaMonkey before 1.0 exposes the internal "AnyName" object to external interfaces, which allows multiple cooperating domains to exchange information in violation of the same origin restrictions.
CVE-2005-4324	Hitachi Groupmax Mail SMTP 06-50 through 06-52-/A and 07-00 through 07-20 allows remote attackers to cause a denial of service (service stop) via an e-mail message with an "invalid format."
CVE-2010-1196	Integer overflow in the nsGenericDOMDataNode::SetTextInternal function in Mozilla Firefox 3.5.x before 3.5.10 and 3.6.x before 3.6.4, Thunderbird before 3.0.5, and SeaMonkey before 2.0.5 allows remote attackers to execute arbitrary code via a DOM node with a long text value that triggers a heap-based buffer overflow.
CVE-2005-2353	run-mozilla.sh in Thunderbird, with debugging enabled, allows local users to create or overwrite arbitrary files via a symlink attack on temporary files.
CVE-2010-3176	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 3.5.x before 3.5.14 and 3.6.x before 3.6.11, Thunderbird before 3.0.9 and 3.1.x before 3.1.5, and SeaMonkey before 2.0.9 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2009-2465	Mozilla Firefox before 3.0.12 and Thunderbird allow remote attackers to cause a denial of service (memory corruption and application crash) or execute arbitrary code via vectors involving double frame construction, related to (1) nsHTMLContentSink.cpp, (2) nsXMLContentSink.cpp, and (3) nsPresShell.cpp, and the nsSubDocumentFrame::Reflow function.
CVE-2014-1577	The mozilla::dom::OscillatorNodeEngine::ComputeCustom function in the Web Audio subsystem in Mozilla Firefox before 33.0, Firefox ESR 31.x before 31.2, and Thunderbird 31.x before 31.2 allows remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read, memory corruption, and application crash) via an invalid custom waveform that triggers a calculation of a negative frequency value.
CVE-2014-1491	Mozilla Network Security Services (NSS) before 3.15.4, as used in Mozilla Firefox before 27.0, Firefox ESR 24.x before 24.3, Thunderbird before 24.3, SeaMonkey before 2.24, and other products, does not properly restrict public values in Diffie-Hellman key exchanges, which makes it easier for remote attackers to bypass cryptographic protection mechanisms in ticket handling by leveraging use of a certain value.
CVE-2011-2373	Use-after-free vulnerability in Mozilla Firefox before 3.6.18 and 4.x through 4.0.1, Thunderbird before 3.1.11, and SeaMonkey through 2.0.14, when JavaScript is disabled, allows remote attackers to execute arbitrary code via a crafted XUL document.
CVE-2012-5835	Integer overflow in the WebGL subsystem in Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0, Thunderbird ESR 10.x before 10.0.11, and SeaMonkey before 2.14 allows remote attackers to execute arbitrary code or cause a denial of service (invalid write operation) via crafted data.
CVE-2011-0084	The SVGTextElement.getCharNumAtPosition function in Mozilla Firefox before 3.6.20, and 4.x through 5; Thunderbird 3.x before 3.1.12 and other versions before 6; SeaMonkey 2.x before 2.3; and possibly other products does not properly handle SVG text, which allows remote attackers to execute arbitrary code via unspecified vectors that lead to a "dangling pointer."
CVE-2013-0750	Integer overflow in the JavaScript implementation in Mozilla Firefox before 18.0, Firefox ESR 10.x before 10.0.12 and 17.x before 17.0.2, Thunderbird before 17.0.2, Thunderbird ESR 10.x before 10.0.12 and 17.x before 17.0.2, and SeaMonkey before 2.15 allows remote attackers to execute arbitrary code via a crafted string concatenation, leading to improper memory allocation and a heap-based buffer overflow.
CVE-2009-3982	Multiple unspecified vulnerabilities in the JavaScript engine in Mozilla Firefox 3.5.x before 3.5.6, SeaMonkey before 2.0.1, and Thunderbird allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2009-0352	Multiple unspecified vulnerabilities in Mozilla Firefox 3.x before 3.0.6, Thunderbird before 2.0.0.21, and SeaMonkey before 1.1.15 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to the layout engine and destruction of arbitrary layout objects by the nsViewManager::Composite function.
CVE-2014-1564	Mozilla Firefox before 32.0, Firefox ESR 31.x before 31.1, and Thunderbird 31.x before 31.1 do not properly initialize memory for GIF rendering, which allows remote attackers to obtain sensitive information from process memory via crafted web script that interacts with a CANVAS element associated with a malformed GIF image.
CVE-2015-2716	Buffer overflow in the XML parser in Mozilla Firefox before 38.0, Firefox ESR 31.x before 31.7, and Thunderbird before 31.7 allows remote attackers to execute arbitrary code by providing a large amount of compressed XML data, a related issue to CVE-2015-1283.
CVE-2008-5012	Mozilla Firefox 2.x before 2.0.0.18, Thunderbird 2.x before 2.0.0.18, and SeaMonkey 1.x before 1.1.13 do not properly change the source URI when processing a canvas element and an HTTP redirect, which allows remote attackers to bypass the same origin policy and access arbitrary images that are not directly accessible to the attacker. NOTE: this issue can be leveraged to enumerate software on the client by performing redirections related to moz-icon.
CVE-2009-1832	Mozilla Firefox before 3.0.11, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.17 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors involving "double frame construction."
CVE-2010-1192	libESMTP, probably 1.0.4 and earlier, does not properly handle a '\0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.
CVE-	The texImage2D implementation in the WebGL subsystem in Mozilla Firefox 4.x through 11.0, Firefox ESR 10.x before 10.0.4,

2012-0478	Thunderbird 5.0 through 11.0, Thunderbird ESR 10.x before 10.0.4, and SeaMonkey before 2.9 does not properly restrict JSVAL_TO_OBJECT casts, which might allow remote attackers to execute arbitrary code via a crafted web page.
CVE-2012-4214	Use-after-free vulnerability in the nsTextEditorState::PrepareEditor function in Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0, Thunderbird ESR 10.x before 10.0.11, and SeaMonkey before 2.14 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors, a different vulnerability than CVE-2012-5840.
CVE-2014-1530	The docshell implementation in Mozilla Firefox before 29.0, Firefox ESR 24.x before 24.5, Thunderbird before 24.5, and SeaMonkey before 2.26 allows remote attackers to trigger the loading of a URL with a spoofed baseURI property, and conduct cross-site scripting (XSS) attacks, via a crafted web site that performs history navigation.
CVE-2012-0446	Multiple cross-site scripting (XSS) vulnerabilities in Mozilla Firefox 4.x through 9.0, Thunderbird 5.0 through 9.0, and SeaMonkey before 2.7 allow remote attackers to inject arbitrary web script or HTML via a (1) web page or (2) Firefox extension, related to improper enforcement of XPConnect security restrictions for frame scripts that call untrusted objects.
CVE-2010-2766	The normalizeDocument function in Mozilla Firefox before 3.5.12 and 3.6.x before 3.6.9, Thunderbird before 3.0.7 and 3.1.x before 3.1.3, and SeaMonkey before 2.0.7 does not properly handle the removal of DOM nodes during normalization, which might allow remote attackers to execute arbitrary code via vectors involving access to a deleted object.
CVE-2009-2466	The JavaScript engine in Mozilla Firefox before 3.0.12 and Thunderbird allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to (1) nsDOMClassInfo.cpp, (2) JS_HashTableRawLookup, and (3) MirrorWrappedNativeParent and js_LockGCThingRT.
CVE-2006-4571	Multiple unspecified vulnerabilities in Firefox before 1.5.0.7, Thunderbird before 1.5.0.7, and SeaMonkey before 1.0.5 allow remote attackers to cause a denial of service (crash), corrupt memory, and possibly execute arbitrary code via unspecified vectors, some of which involve JavaScript, and possibly large images or plugin data.
CVE-2007-3699	The Decomposer component in multiple Symantec products allows remote attackers to cause a denial of service (infinite loop) via a certain value in the PACK_SIZE field of a RAR archive file header.
CVE-2013-0776	Mozilla Firefox before 19.0, Firefox ESR 17.x before 17.0.3, Thunderbird before 17.0.3, Thunderbird ESR 17.x before 17.0.3, and SeaMonkey before 2.16 allow man-in-the-middle attackers to spoof the address bar by operating a proxy server that provides a 407 HTTP status code accompanied by web script, as demonstrated by a phishing attack on an HTTPS site.
CVE-2014-1593	Stack-based buffer overflow in the mozilla::FileBlockCache::Read function in Mozilla Firefox before 34.0, Firefox ESR 31.x before 31.3, Thunderbird before 31.3, and SeaMonkey before 2.31 allows remote attackers to execute arbitrary code via crafted media content.
CVE-2012-4213	Use-after-free vulnerability in the nsEditor::FindNextLeafNode function in Mozilla Firefox before 17.0, Thunderbird before 17.0, and SeaMonkey before 2.14 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2014-1490	Race condition in libssl in Mozilla Network Security Services (NSS) before 3.15.4, as used in Mozilla Firefox before 27.0, Firefox ESR 24.x before 24.3, Thunderbird before 24.3, SeaMonkey before 2.24, and other products, allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via vectors involving a resumption handshake that triggers incorrect replacement of a session ticket.
CVE-2009-2408	Mozilla Network Security Services (NSS) before 3.12.3, Firefox before 3.0.13, Thunderbird before 2.0.0.23, and SeaMonkey before 1.1.18 do not properly handle a '\0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority. NOTE: this was originally reported for Firefox before 3.5.
CVE-2014-1552	Mozilla Firefox before 31.0 and Thunderbird before 31.0 do not properly implement the sandbox attribute of the IFRAME element, which allows remote attackers to bypass intended restrictions on same-origin content via a crafted web site in conjunction with a redirect.
CVE-2010-1194	The match_component function in smtp-tls.c in libESMTP 1.0.3.r1, and possibly other versions including 1.0.4, treats two strings as equal if one is a substring of the other, which allows remote attackers to spoof trusted certificates via a crafted subjectAltName.
CVE-2015-2737	The rx::d3d11::SetBufferData function in the Direct3D 11 implementation in Mozilla Firefox before 39.0, Firefox ESR 31.x before 31.8 and 38.x before 38.1, and Thunderbird before 38.1 reads data from uninitialized memory locations, which has unspecified impact and attack vectors.
CVE-2009-1833	The JavaScript engine in Mozilla Firefox before 3.0.11, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.17 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to (1) js_LeaveSharpObject, (2) ParseXMLSource, and (3) a certain assertion in jsinterp.c; and other vectors.
CVE-2011-2374	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 3.6.18 and 4.x through 4.0.1, and Thunderbird before 3.1.11, allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2012-1937	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 4.x through 12.0, Firefox ESR 10.x before 10.0.5, Thunderbird 5.0 through 12.0, Thunderbird ESR 10.x before 10.0.5, and SeaMonkey before 2.10 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.